FLUKE networks

AirCheck™

Wi-Fi Tester

Users Manual

January 2010, Rev. 2 4/11
©2010-2011 Fluke Corporation. All rights reserved.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the WiFi Alliance.

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Each Fluke Networks product is warranted to be free from defects in material and workmanship under normal use and service. The warranty period for the mainframe is one year and begins on the date of purchase. Parts, accessories, product repairs and services are warranted for 90 days, unless otherwise stated. Ni-Cad, Ni-MH and Li-Ion batteries, cables or other peripherals are all considered parts or accessories. The warranty extends only to the original buyer or end user customer of a Fluke Networks authorized reseller, and does not apply to any product which, in Fluke Networks' opinion, has been misused, abused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke Networks warrants that software will operate substantially in accordance with its functional specifications for 90 days and that it has been properly recorded on non-defective media. Fluke Networks does not warrant that software will be error free or operate without interruption.

Fluke Networks authorized resellers shall extend this warranty on new and unused products to end-user customers only but have no authority to extend a greater or different warranty on behalf of Fluke Networks. Warranty support is available only if product is purchased through a Fluke Networks authorized sales outlet or Buyer has paid the applicable international price. Fluke Networks reserves the right to invoice Buyer for importation costs of repair/replacement parts when product purchased in one country is submitted for repair in another country.

Fluke Networks warranty obligation is limited, at Fluke Networks option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke Networks authorized service center within the warranty period.

To obtain warranty service, contact your nearest Fluke Networks authorized service center to obtain return authorization information, then send the product to that service center, with a description of the difficulty, postage and insurance prepaid (FOB destination). Fluke Networks assumes no risk for damage in transit. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB destination). If Fluke Networks determines that failure was caused by neglect, misuse, contamination, alteration, accident or abnormal condition of operation or handling, or normal wear and tear of mechanical components, Fluke Networks will provide an estimate of repair costs and obtain authorization before commencing the work. Following repair, the product will be returned to the Buyer transportation prepaid and the Buyer will be billed for the repair and return transportation charges (FOB Shipping point).

THIS WARRANTY IS BUYER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY.

Since some countries or states do not allow limitation of the term of an implied warranty, or exclusion or limitation of incidental or consequential damages, the limitations and exclusions of this warranty may not apply to every buyer. If any provision of this Warranty is held invalid or unenforceable by a court or other decision-maker of competent jurisdiction, such holding will not affect the validity or enforceability of any other provision.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Contents

Title	Page
Introduction	1
Registering Your Product	1
The Fluke Networks Knowledge Base	1
Contact Fluke Networks	2
Safety Information	2
Unpacking	3
AirCheck Wi-Fi Tester	3
AirCheck Frontline Troubleshooting Kit	3
Physical Features	4
Battery Charging and Life	6
Minimum Configuration for the Best Performance	7
What You Can Learn About Your Network	8
What is in the Wireless LAN?	8
Can Devices Connect to the Network?	9
What Causes Slow Network Performance or Dropped Connections?	10
Are There Security Risks in the Network?	11
What Networks or Access Points Come into Range as I Move?	12
How Can I Document My Network and My Test Session?	12
Where is an Access Point?	12

The Home Screen 13
Set Up the Tester 14
    Change the Language and Country Settings 14
    Make a Profile to Connect to Secure Networks 14
    Settings 16
    802.11d Operation 20
    Change the Thresholds for the Colors in Bar Graphs 21
    Give Access Points an Authorization Status 22
Discover Networks and Access Points 23
If the Tester Does Not Discover an Access Point 34
Notes for Networks and Access Points 35
Channel Usage 38
Verify Connectivity 41
    Load a Profile that Includes Security Credentials 42
    Connect to a Network or Access Point 42
    Ping a Device or Web Server 46
Discover Clients 49
If the Tester Does Not Discover a Client 54
Locate an Access Point or a Client 54
The External Directional Antenna 58
Adjust Signal Strength Measurements to Agree with Other Devices 61
Save a Test Session 62
Manage Files on the Tester 63
    About Files on the Tester 64
    Transfer Files to a PC 65
Maintenance 65
    Clean the Tester 66
    Update the Software in the Tester 66

Restore Factory Defaults 67
Device Information 67
If the Tester Will Not Turn Off 67
Options and Accessories 67
Specifications 69
Environmental Specifications 69
General Specifications 71
Wireless Specifications 72
Federal Communication Commission and Industry Canada Interference Statement 75
Important Note: FCC and IC Radiation Exposure Statement 75
Europe-EU Declaration of Conformity 76
Appendix A: Log Messages for Connections that Fail 79
Appendix B: Default Settings 83
Appendix C: 802.11d Country Codes 85
Index 95

List of Figures

Figure		Page
1.	Physical Features	4
2.	How to Remove the Battery	6
3.	The Home Screen	13
4.	Change the Thresholds for the Colors in a Bar Graph	21
5.	Networks (SSIDs) List	24
6.	Access Points List	28
7.	Access Point Details Screen	32
8.	Channel Usage Screen	39
9.	Channel Usage Details Screen	40
10.	The Connection Screen	44
11.	The Connection Log	45
12.	The Ping Screen	47
13.	Clients Screen	50
14.	Client Details Screen	52
15.	Locate Access Point Screen	55
16.	Locate Client Screen	56
17.	Search Pattern for the Omnidirectional Antenna in the Tester	57
18.	Search Pattern for the External Antenna	59
19.	How to Point the External Antenna	60
20.	Antenna Patterns for the External Antenna (magnitude (dBi)) vs. azimuth (degrees)	74

AirCheck™ Wi-Fi Tester

Introduction

The AirCheck™ Wi-Fi Tester lets you make sure that 802.11 wireless LANs are available to mobile users, examine the usage of channels to help you do an analysis of network health, and find the source of connection problems. The tester operates on 802.11 b/g/n networks in the 2.4 GHz band and 802.11 a/n networks in the 5 GHz band.

The optional PoE detector shows you if Power over Ethernet voltage from 802.3af and higher-power 802.3at devices is available on twisted pair network cabling.

You can save the test results and use AirCheck™ Manager software to transfer the results to a PC and make professional-quality reports. You can use AirCheck Manager to compare information from different test sessions to see changes in a wireless LAN.

Registering Your Product

Registering your product with Fluke Networks gives you access to valuable information on product updates, troubleshooting procedures, and other services. To register, fill out the online form on the Fluke Networks website at **www.flukenetworks.com/registration**.

The Fluke Networks Knowledge Base

The Fluke Networks Knowledge Base gives answers to common questions about Fluke Networks products and includes information on technology and procedures for network and cable tests. To see the Knowledge Base, go to **www.flukenetworks.com**, then click **Support** > **Knowledge Base**.

Contact Fluke Networks

www.flukenetworks.com
support@flukenetworks.com
+1-425-446-4519

- Australia: 61 (2) 8850-3333 or 61 (3) 9329 0244
- Beijing: 86 (10) 6512-3435
- Brazil: 11 3759 7600
- Canada: 1-800-363-5853
- Europe: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japan: 03-6714-3117
- Korea: 82 2 539-6311
- Singapore: +65-6799-5566
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853

For more phone numbers, go to our website.

Safety Information

Table 1 gives descriptions of the safety symbols used on the tester and in this manual.

Table 1. Safety Symbols

	Warning or Caution: risk of damage to or destruction of equipment or software. See explanations in the manual.
	Warning: Risk of electrical shock.
	Do not put products that contain circuit boards into waste containers. Refer to local regulations for disposal procedures.
	This equipment contains a Class 2 radio.

⚠Warning⚠

Use only the ac adapter provided to charge the battery.

⚠Caution

If you use an external antenna, use only the antenna that Fluke Networks makes for the AirCheck tester. The tester will not operate correctly with other antennas.

Unpacking

The AirCheck Wi-Fi Tester comes with the accessories in the list below. If something is damaged or missing, tell the dealer where you purchased the product.

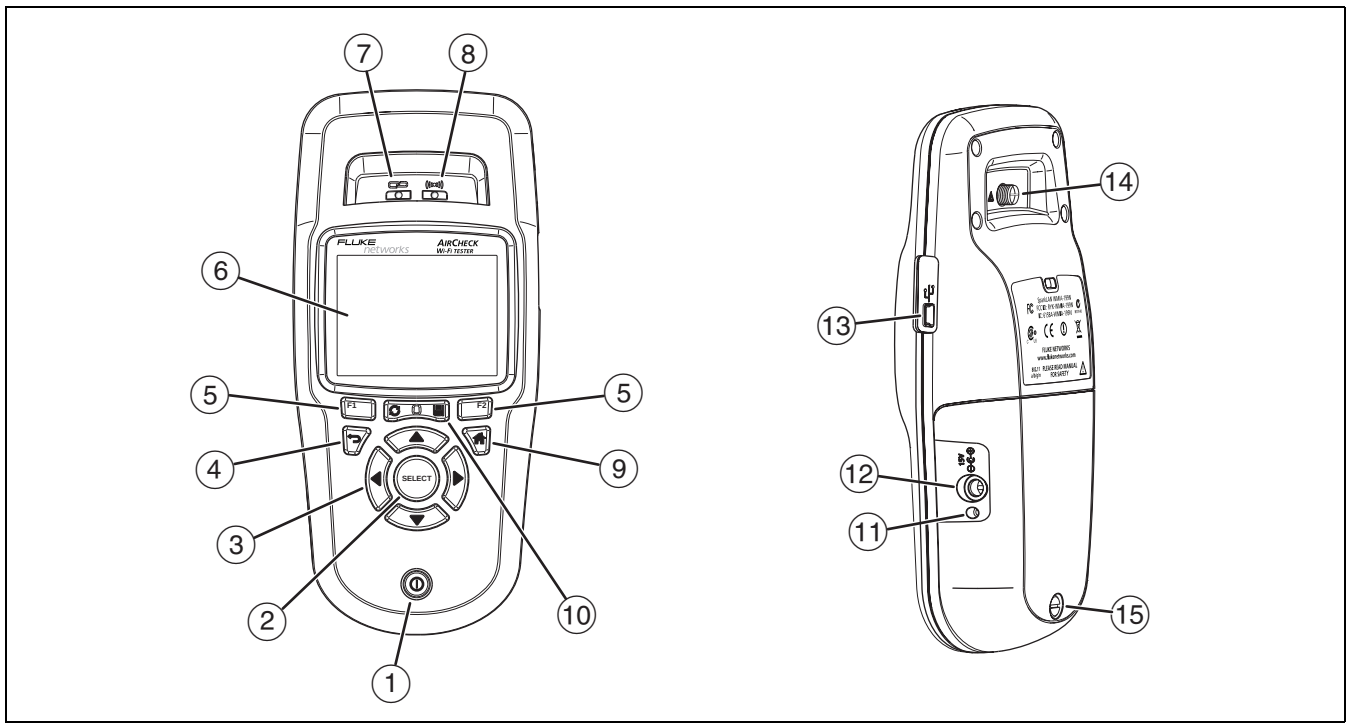
AirCheck Wi-Fi Tester

- AirCheck with rechargeable battery pack
- AC adapter
- USB cable
- Carrying case
- Getting Started Guide
- Product manuals CD
- AirCheck Manager Software CD

AirCheck Frontline Troubleshooting Kit

- AirCheck with rechargeable battery pack
- Extra battery pack
- LinkRunner™ Pro
- External directional antenna with RSMA connector
- PoE detector
- AC adapter
- USB cable
- Carrying case
- Getting Started Guide
- Product manuals CD
- AirCheck Manager Software CD

Physical Features



ffy01.eps

Figure 1. Physical Features

① On/off key.

② Makes a selection on the screen.

③ Navigation keys.

④ Shows the previous screen.

⑤ Softkeys. The function of the softkey is shown above the key.

⑥ Full-color LCD.

⑦ The LED blinks when the tester tries to connect to a wireless LAN. The LED is on when the tester is connected to a wireless LAN.

⑧ The LED blinks when the tester transmits data.

⑨ Shows the home screen.

⑩ : Erases all data collected during the current sequence of tests. This does not erase the results saved in memory.
: Saves all data in a session file. See page 62.

⑪ The LED turns on when you connect the ac adapter. The LED is red when the battery charges and green when the battery is fully charged.

⑫ Connector for the ac adapter.

⑬ USB port for connection to a PC.

⑭ Connector for the external directional antenna. See page 58.

⑮ Screw for the battery pack.

Battery Charging and Life

Charge the battery for 4 hours before you use it for the first time.

To charge the battery, connect the ac adapter to the battery connector (⑫ in Figure 1). You can use the tester while you charge the battery.

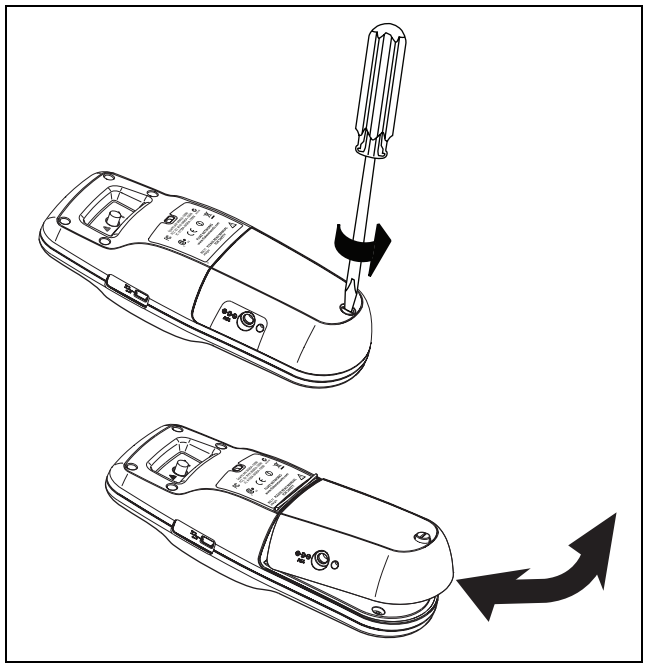
Figure 2 shows how to replace the battery.

When the tester is off, the battery charges in approximately 3 hours.

Note

The battery will not charge if the internal temperature of the tester is above 113°F (45°C).

The battery life is approximately 5.5 hours during typical operation. An icon in the upper-left corner of the screen shows the battery status. See Figure 3 on page 13.



ffy14.eps

Figure 2. How to Remove the Battery

Minimum Configuration for the Best Performance

To get the most performance from your tester, use AirCheck Manager to configure a profile and transfer it to the tester. A profile contains data that lets the tester do these tasks:

- Connect to networks that require security credentials
- Show the correct authorization status for each access point. This lets you quickly see which access points are authorized parts of the network.
- Ping key network devices.

See “Set Up the Tester” on page 14.

What You Can Learn About Your Network

The sections below give an overview of what the tester can tell you about a network.

What is in the Wireless LAN?

What wireless LANs are available?	Select **Networks** to see a list of wireless LANs and the access points that connect to each network. To see all access points that are available at your location, select **Access Points**. See page 24.
What access points are available? Are the signal strengths sufficient?	Select **Access Points** to see a list of access points available at your location and the signal strength of the access points. See page 28.
Is the access point configured correctly?	Select **Access Points**, highlight an access point, then press SELECT. See page 28.
Are there new access points in the area? Are access points inaudible?	Save the test session, then use AirCheck Manager to compare the access point list to another list saved in AirCheck Manager. See pages 54 and 65.
What wireless clients use the network?	Select **Tools**, then select **List clients**. See page 49.

Can Devices Connect to the Network?

Use the tester to verify connectivity.

Note

To connect to a secure network, the tester must have a profile that includes security credentials. If credentials are not available, the softkey shows as F1 ***Connect*.*** *See page 14.*

Can a device connect as a client to the network (SSID)?	Select **Networks**, highlight a network, then press F1 **Connect**. See page 42.
Can a device connect to an access point (BSSID)?	Select **Access Points**, highlight an access point, then press F1 **Connect**. See page 42.
If a device cannot connect to a network or access point, where does the connection procedure fail?	Look at the connection log. See page 45.
Can a device ping a network device?	Do a ping test. See page 46.
Does the network interface card in a client operate correctly?	Select **Tools**, then select **List clients** to see if the client transmits probe request frames and to see basic settings such as the channel and SSIDs the client uses in probes. See page 50.

What Causes Slow Network Performance or Dropped Connections?

Is the signal strength sufficient?	Select **Access Points**. The **Access Points** screen shows the signal strength for each access point. Select an access point to see more details about the signal strength and congestion. See page 32.
Is the network too busy?	Select **Channels** to see an overview of channel usage and the number of access points that use each channel. To see a graph, highlight a channel, then press SELECT. See page 39.
Do too many clients use a channel or access point?	Select **Tools**, then select **List clients** to see how many clients use a channel or AP. See page 49.
Do too many clients use a low data rate?	Select **Tools**, then select **List clients** to see data rates for clients. See page 49.
Is there non-802.11 interference on a channel?	Select **Channels**. Non-802.11 interference is gray. This noise can interfere with WLAN connections or performance. Non-802.11 noise can come from microwave ovens, wireless telephones, Bluetooth® devices, motion detectors, wireless cameras and other wireless devices. See page 40.

Are There Security Risks in the Network?

Do networks have the expected level of security?	Select **Networks**. Networks that have unsecured access points show a red open lock ( ). See page 24.
Are there any ad hoc networks in the area?	Select **Networks**. Networks that have ad hoc clients show the ad hoc icon ( ) in the **SSID** column. Ad hoc clients can be risks to network security or can violate network policies. See page 24.
Are there rogue access points in the area? Where are they?	Access points have the status " **Unauthorized device**" until you change the status. If you give all access points in the network a status, then new access points that can be rogues show the status . If you know that an access point is a rogue, you can give it the status " **Flagged Device"**. See page 22. To give an authorization status, select **Access Points**, highlight an access point, then press F2 **ACL**. To locate an access point, select it, then press F2 **Locate** on the **Access Point Details** screen. See page 54.

Where is an Access Point?

Select **Access Points**, select one access point, then press F2 **Locate** on the **Access Point Details** screen. See page 54. Use the optional Fluke Networks external directional antenna to help you find access points faster. See page 54.

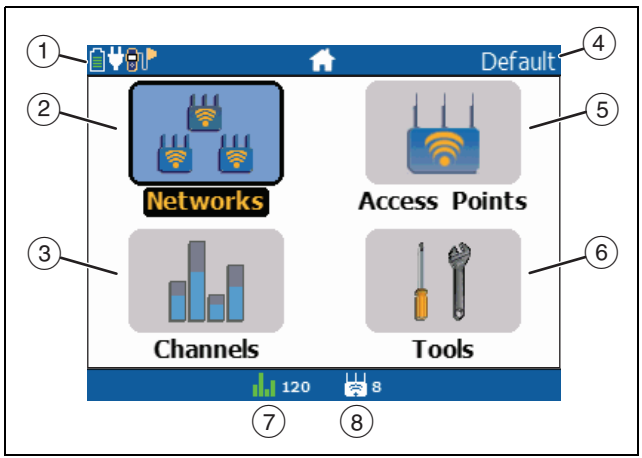
What Networks or Access Points Come into Range as I Move?

Sort the list in descending sequence for the timestamp column (). Press , then move through an area. Networks or access points that come into range are added to the top of the list. See page 25 or 29.

How Can I Document My Network and My Test Session?

Save the session (see page 54), then use AirCheck Manager software to transfer the data to a PC and make a report. See page 65.

The Home Screen



ffy15.eps

Figure 3. The Home Screen

1 Shows the battery status. When the battery charge is low, the icon blinks. Connect the ac adapter to charge the battery and to make sure the tester continues to operate.

Shows that the ac adapter is connected.

Shows that the external antenna is connected.

2 **Networks**: Discovers wireless LANs. See page 23.

3 **Channels**: Shows usage of WLAN channels. See page 38.

4 The name of the profile the tester uses. The profile is **Default** if you have not loaded a different profile. The name shows an asterisk if you have changed a setting on the tester since you loaded or saved the profile. See page 64.

5 **Access Points**: Discovers access points. See page 23.

6 **Tools**: Lets you manage files and settings. Also lets you see a list of clients that transmit probes (see page 49).

7 The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See “802.11d Operation” on page 20

8 The number of access points the tester has found. This number does not include virtual access points if **Group virtual access points** is selected. See page 17.

Set Up the Tester

To change settings on the tester, select **Tools** from the home screen. See Table 2 on page 17.

Change the Language and Country Settings

1 Select **Tools**.

2 To change the language for the screens, select **Set Language**. Highlight a language, then press F2 **Save.**

3 To change the country, select **Set Country**, then select the country where you will use the tester. See page 19.

Make a Profile to Connect to Secure Networks

Profiles are files that contain settings for networks and the tester. The network settings include security credentials. Security credentials let the tester connect to networks and do ping tests. Profiles can have passwords so that unauthorized users do not have access to network security credentials in AirCheck Manager and cannot use the tester to connect to secure networks.

You can save the settings from the tester as a profile or use AirCheck Manager to make a profile on a PC.

The home screen shows the name of the profile the tester uses. The name shows an asterisk if you have changed a setting on the tester since you loaded or saved the profile. The tester saves the changes in a temporary file, which is a copy of the profile shown on the home screen. The tester uses the temporary file as the current profile. When you save the profile, the tester copies the changes into the profile shown on the home screen.

Profiles that you make in AirCheck Manager include these settings:

- A password for the profile
- Security credentials for networks

  Note

  To make a profile that includes security credentials for a network or a password for the profile, you must use AirCheck Manager.

- IP addresses and the authorization status of networks (SSIDs) and access points
- IP addresses used for ping tests
- All 802.11 settings (For example, **Enable 2.4 GHz band** and **Enable 5 GHz band.** See page 17.)

- Country
- Threshold settings for bar graphs

If you save the profile while you use it on the tester, the tester adds these settings to the profile:

- The sound setting for the locate function
- The auto shutoff setting
- Sequences for the sort order for lists of networks, access points, and clients

To transfer a profile from a PC to the tester

1 Use the **Profile Manager** in AirCheck Manager to make a profile.

2 Use the USB cable supplied with the tester to connect the tester to the PC.

3 Use the transfer function in the **Profile Manager** to transfer the profile to the tester.

To load a profile that is in the tester

1 Select **Tools** > **Manage files**, then select **Load profile**.

2 Highlight a profile, press SELECT, then press F2 **Load**.

Note

If the file is not a valid profile, or if the extension is not ".ACP", the tester shows the message ***"Unable to load selected profile"****.*

3 Enter the password for the profile, if necessary.

Note

You must enter the password only the first time you load a profile on the tester. To put password protection on all profiles again, select ***Tools*** *>* ***Restore factory defaults****.*

To save the current settings as a profile

1 Select **Tools** > **Manage files**, then select **Save profile**.

- To save the profile with the filename shown, press F2 **Save**. The tester saves the profile in the "PROFILES" folder.
- To overwrite a profile that is saved on the tester, highlight the profile, press SELECT, press F2 **Save**, then press F2 **OK**.
- To edit the filename, press F1 **Edit**.

-continued-

Note

File names can have a maximum of 8 characters with an extension of 3 characters. The extension must be ".ACP" if you want to see the profile in AirCheck Manager.

- To delete characters in the filename, press F1 **Delete**.
- To add characters to the filename, use ◄ ► ▲ ▼ to highlight a character, then press SELECT.
- To move the cursor in the filename, highlight the filename, then press ◄ ►.
- To save the profile with the edited filename, press F2 **Done**, then press F2 **Save**. The tester saves the profile in the "PROFILES" folder.

Settings

Table 2 shows the settings you can make on the **Tools** menu.

When you change a setting, press F2 **Save** to save your changes. To exit and not save your settings, press F1 **Cancel**.

Note

*To save your settings in a profile, select **Tools** > **Save profile**.*

Table 2. Settings on the Tools Menu

Manage 802.11 settings *Note* *These settings change how the tester finds and displays access points. Make sure that you know what these settings do before you use the tester.*	Lets you set options for channels and access point lists. • **Enable 2.4 GHz band, Enable 5 GHz band**: Select one or both frequency bands to see networks and access points from one or both bands. • **Transmit probes**: To discover access points, the tester listens for SSID broadcasts on each channel. The tester can discover only access points that broadcast their SSID while the tester is on the same channel. For faster discovery, the tester transmits probe request frames by default to get responses from access points. Because probes increase channel usage, the tester does not transmit them when you look at the channel usage screens or when you connect the external antenna.

-continued-

Table 2. Settings on the Tools Menu (continued)

Manage 802.11 settings (continued) *Note* *These settings change how the tester finds and displays access points. Make sure that you know what these settings do before you use the tester.*	• **Group virtual access points**: When an access point broadcasts multiple MAC addresses (**BSSIDs)**, the MACs are virtual access points. Virtual access points can support different networks from the same physical access point. An access point that uses two radios to broadcast multiple MACs can support networks on different channels. When **Group virtual access points** is enabled, virtual access points show as one access point in the **Access Points** list. If the access point broadcasts a name (shown in the **Name/MAC** column), the number of SSIDs it supports shows in the **SSID** column. For example, "**2 SSIDs**" shows in the column. If the access point does not broadcast a name, it has an asterisk as the last digit of the MAC address in the **Name/MAC** column. To see the MAC addresses an**d SSIDs** for the virtual access points, select the access point in the **Access Points** list. By default, this setting is enabled. • **Gray inaudible access points:** If the tester has not heard an access point for four cycles through all channels, the access point is gray in the **Access Points** list. This is the default setting. • **Delete inaudible access points**: If the tester has not heard an access point for four cycles through all channels, it deletes the access point from the **Access Points** list.

Table 2. Settings on the Tools Menu (continued)

Use custom signal adjustment	Lets you adjust signal strength measurements to agree with other devices. See page 61.
Set time and date	Lets you set the time and date, which the tester includes with saved results. Use ◀ ▶ to select a setting, then use ▼ ▲ to change the setting.
Set thresholds	Lets you set the thresholds for the colors in measurement bar graphs. See page 21.
Set country	Channels that are illegal in the country you select are red on the **Channel Usage**, **Channel Usage Details**, and **Access Point Details** screens. See "802.11d Operation" on page 20. Access points that transmit a country code that does not agree with this setting have red bars in the **802.11** column.
Set language	Sets the language for the user interface.
Manage power	When you enable this, the tester turns off automatically if you do not press a key for 10 minutes. The tester does not save the test session when it turns off automatically. It does save changes you made to the profile. The tester does not turn off automatically if the ac adapter is connected. To save your setting, press F2 **Save.** To exit and not save your setting, press F1 **Cancel**.
Restore factory defaults	Makes all settings go back to default values. See Appendix B.

802.11d Operation

If an access point uses the 802.11d standard, it transmits an ISO country code in its beacons and probe responses. When the tester receives this code, it transmits only on channels that are legal in the country, and uses only power levels that are legal.

If the tester does not receive a country code, the tester operates in "world mode":

- The tester uses only channels and power levels that are legal in all countries. The channels are 1 to 11 in the 2.4 GHz band.
- The tester will not transmit probes on channels 12, 13, and 14 in the 2.4 GHz band.
- The tester will not transmit in the 5 GHz band unless it sees access points that operate in that band.
- The tester uses the lowest transmission power that is legal in all countries.

The bars at the bottom of the display and icons on the networks and access point displays show the status of the country code:

Green bars: The tester received a country code from one or more access points. All country codes received are the same, and they all agree with the setting in **Tools** > **Set country**. The tester operates on channels and uses power levels that are legal in that country.

White bars: The tester has not received a country code. The tester operates in world mode.

Red bars: The tester received a country code that is different from the setting in **Tools** > **Set country**. To identify the network or access point that transmits the code, select **Networks** or **Access Points**, then look for the red bars in the **802.11** column.

The **Access Point Details** screen shows the 802.11d country code that the access point transmits. Appendix C shows the countries for the codes.

Change the Thresholds for the Colors in Bar Graphs

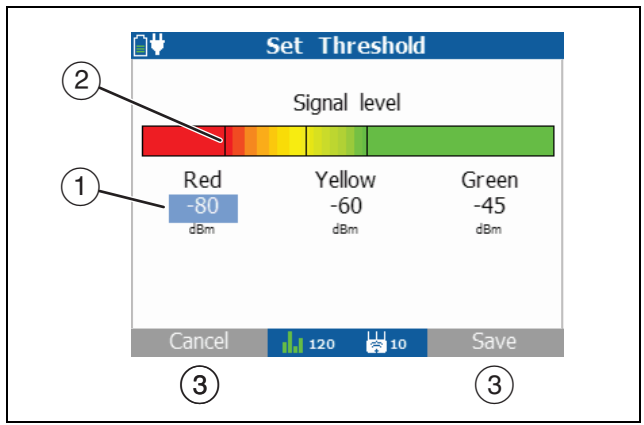
The colors of bar graphs show you if the signal strength, noise, and signal to noise ratio are above or below specified thresholds. You can change the thresholds so that the colors show you if the signal meets the requirements of your network.

To change thresholds for the colors

1 Select **Tools**.

2 Select **Set thresholds**.

3 Select an item. Figure 4 shows how to change the thresholds for the colors.



ffy05.eps

Figure 4. Change the Thresholds for the Colors in a Bar Graph

(1) Use ◄► to select a color. Use ▲▼ to increase or decrease the measured value for the color.

(2) The lines show where the value you set is on the bar graph.

(3) To save your settings, press F2 **Save**. To exit and not save your settings, press F1 **Cancel**.

Give Access Points an Authorization Status

When you set the authorization status for each access point, you can quickly see if an access point is an authorized part of the network. Access points have the yellow triangle (⚠) in the access control list column (**ACL**) until you change the status.

To give an access point an authorization status

1 Select **Access Points**.

2 If an access point has more than one MAC address and you want to give the MACs different authorization statuses, select the access point.

3 Highlight an access point, then press F2 **ACL**.

4 Highlight a status on the **Authorization Status** screen, press SELECT, then press ↵.

⚠ **Unauthorized device**: The access point does not have an authorization status.

✓ **Authorized device**: The access point is authorized to connect to the network.

Neighbor device: The access point is not authorized to connect to the network, but is not a threat to network security.

Guest device: The access point is authorized to connect to the network, but has limited access.

Flagged device: You can use this symbol for access points you want to monitor. For example, if you think that an access point is a rogue, you can put a flag on it until you learn more about it.

When you turn off the tester, it saves the ACL settings in the temporary profile.

Note

If an access point does not transmit, but you know its MAC address, you can use AirCheck Manager to give the access point an authorization status. Save the status in a profile, then transfer the profile to the tester.

Discover Networks and Access Points

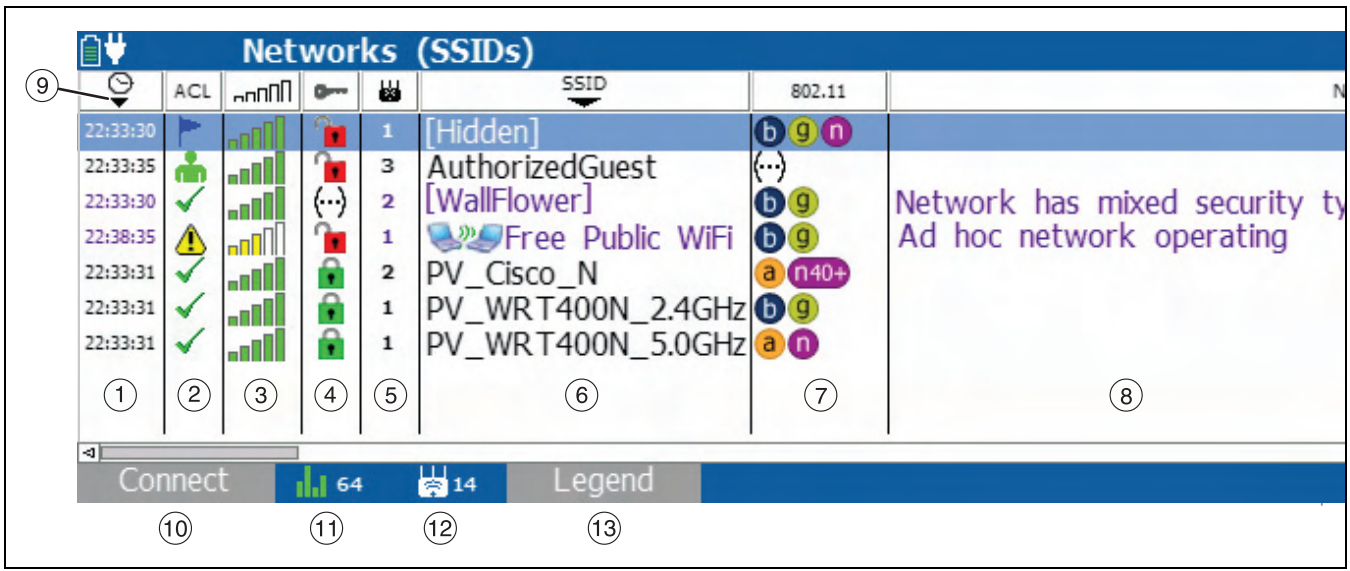
Note

By default, the tester looks for wireless signals on the 2.4 GHz (b/g/n) and 5 GHz (a/n) frequency bands to identify wireless access points. To change this setting, select ***Tools****, then select* ***Manage 802.11 settings****.*

To discover networks or access points

1. From the home screen, select **Networks** or **Access Points**. The tester shows the **Networks** list or **Access Points** list (Figures 5 and 6).

2. To see details about an access point (Figure 7), use ◁▷ to highlight the access point, then press SELECT.



ffy03.eps

Figure 5. Networks (SSIDs) List

① : The time when the tester first heard the network. To see networks that come into range as you move through an area, sort the list in descending sequence for the timestamp column.

Press , then move through an area. Networks that come into range are added to the top of the list. Networks that become out of range become gray if **Gray inaudible access points** is enabled.

② **ACL**: The authorization status of the access point. The default status is **Unauthorized device**. Change the status of each access point to show how it is related to your network. See page 22.

(...): All access points in the network do not have the same authorization status.

③ : The maximum signal strength of all the access points for a network **SSID**. You can change the thresholds for the colors in the bar graphs. See page 21.

④ : The security status of the network:

Red open lock: The network does not have security enabled.

Yellow closed lock: One or more access points use WEP or Cisco LEAP security protocol. These are less secure than other protocols.

Green closed lock: All access points use security protocols that are more secure than WEP, for example, WPA or WPA2.

(...): All access points in the network do not use the same type of security. For example, one uses WEP and another uses WPA.

⑤ : The number of access points the tester hears at your location.

⑥ **SSID**: Service Set Identifier. The name of the wireless network.

Networks that the tester has not heard recently are gray if **Gray inaudible access points** is enabled (see page 18).

: The network has ad hoc devices. These are devices that communicate directly with other devices, not through an access point that is part of the network. Ad hoc devices can give hackers access to data transmitted on the network. (Some IT policies for networks allow ad hoc devices.)

[Hidden]: The network does not broadcast its SSID.

If an SSID shows in square brackets, the tester found the hidden SSID in packets from other wireless clients. In AirCheck Manager, these SSIDs show without square brackets.

⑦ **802.11**: The 802.11 standards that the access points in the network use:

802.11a: Uses the 5 GHz band.

802.11b: Uses the 2.4 GHz band.

802.11g: Uses the 2.4 GHz band.

802.11n: Can be used in the 2.4 GHz or 5 GHz bands.

Red bars: The tester received a 802.11d country code from the access point. The country does not agree with the country selected in **Tools** > **Set country** in the tester.

n40+ n40–: One or more access points use a bonded channel. Access points that use the 802.11n standard can bond a channel with an extension channel above (n40+) or below it (n40–) to make one 40 MHz channel. This wider channel gives the network higher throughput.

(...): All access points in the network do not use the same 802.11 standard.

⑧ **Notes**: Press ▶ to scroll to the notes field. The tester adds notes automatically. See page 35. Networks that have notes are purple.

(...): The network has multiple notes. To see all notes, highlight the network, then press SELECT twice to go to the **Access Point Details** screen.

⑨ ▼▲: **Sort 1**, descending and ascending sequences

▼ ▲ : **Sort 2**, descending and ascending sequences

To sort the list in ascending or descending sequence, use ◀ and ◀ ▶ to highlight a column heading, then press SELECT or F1 **Sort 1**. For example, to quickly find the access point that has the strongest signal, highlight ▁▃▅▇ at the top of the column, then press SELECT or F1 **Sort 1**. This puts the access point with the strongest signal at the top of the list.

To sort in a secondary sequence, highlight a different column heading, then press F2 **Sort 2**.

⑩ Press F1 **Connect** to connect to the highlighted network. See page 42.

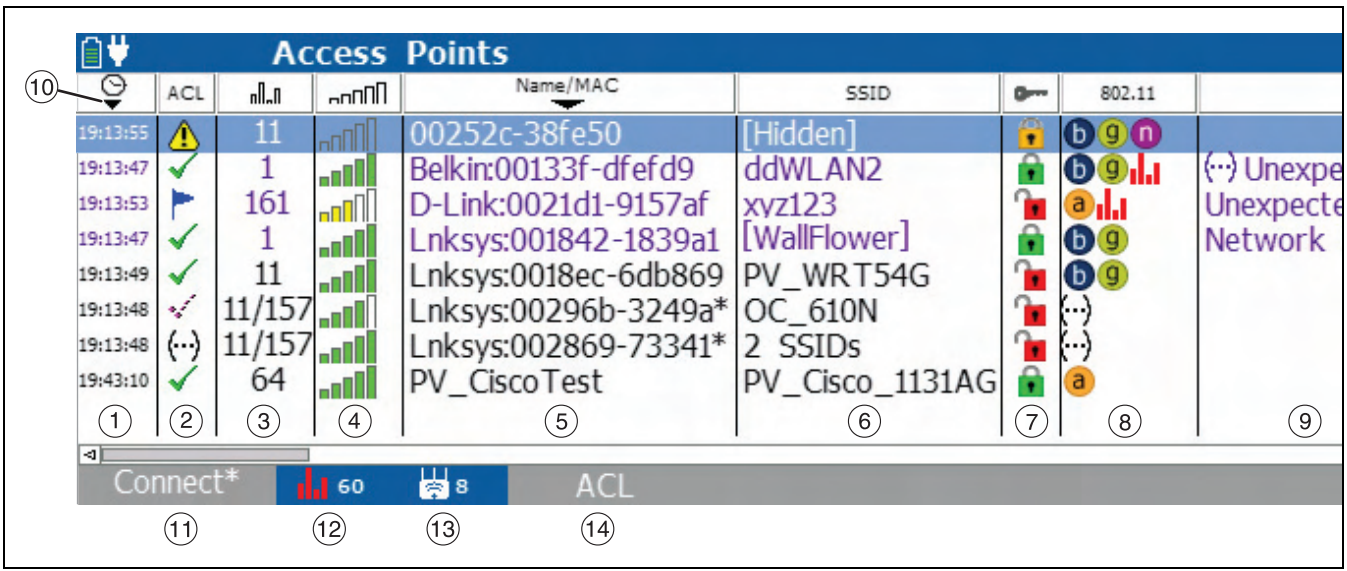
The connect button shows as "**Connect***" if the tester cannot connect to the highlighted network. See page 42.

⑪ : The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See “802.11d Operation” on page 20.

⑫ : The number of access points the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected. See page 17.

⑬ To see descriptions of the icons on the **Networks** screen, press F2 **Legend**.

To see details about the access points in a network, use ▲ ▼ to highlight a network, then press SELECT. See Figure 6.



ffy02.esp

Figure 6. Access Points List

① : The time when the tester first heard the access point. To see access points that come into range as you move through an area, sort the list in descending sequence for the timestamp column.

Press , then move through an area. Access points that come into range are added to the top of the list. Access points that go out of range become gray if **Gray inaudible access points** is enabled.

② **ACL**: The authorization status of the access point. The default status is **Unauthorized device**. Change the status of each access point to show how it is related to your network. See page 22.

(...): Virtual access points or MACs from the same access point have different authorization status settings. Usually, you give them the same authorization status.

③ : The channel that the access point uses.

④ : The strength of the signal. For multiple APs, this column shows the strength of the strongest signal. You can change the thresholds for the colors in the bar graphs. See page 21.

⑤ **Name/MAC**: The name or MAC address of the access point. The address starts with a vendor abbreviation prefix, if the prefix is available. See "oui_abbr.txt" on page 64.

*****: The access point broadcasts more than one MAC address (BSSID). To see the MAC addresses, select the access point. See "**Group virtual access points**" on page 18.

Access points that the tester has not heard recently are gray if **Gray inaudible access points** is enabled (see page 18).

⑥ **SSID**: Service Set Identifier. The name of the wireless network.

If the access point supports more than one SSID, select the access point to see the SSIDs. See "**Group virtual access points**" on page 18.

If you came to this screen from the **Networks** screen, the screen shows the SSID at the top.

Networks that the tester has not heard recently are gray if **Gray inaudible access points** is enabled (see page 18).

: The network has ad hoc devices. These are devices that communicate directly with other devices, not through an access point that is part of the network. Ad hoc devices can give hackers access to data transmitted on the network. (Some IT policies for networks allow ad hoc devices.)

[Hidden]: The network does not broadcast its SSID.

If an SSID shows in square brackets, the tester found the hidden SSID in packets from other wireless clients. In AirCheck Manager, these SSIDs show without square brackets.

⑦ : The security status of the access point:

Red open lock: The access point does not have security enabled.

Yellow closed lock: The access point uses WEP security protocol.

Green closed lock: The access point uses a security protocol that is more secure than WEP, for example, WPA or WPA2.

: The access point is an ad hoc device. These are devices that communicate directly with other devices, not through an access point that is part of the network. Ad hoc devices can give hackers access to data transmitted on the network. (Some network policies allow ad hoc devices.)

(...): All access points do not use the same type of security. For example, one uses WEP and another uses WPA.

⑧ **802.11**: The 802.11 standards that the access point uses:

: 802.11a: Uses the 5 GHz band.

: 802.11b: Uses the 2.4 GHz band.

: 802.11g: Uses the 2.4 GHz band.

: 802.11n: Can be used in the 2.4 GHz or 5 GHz bands.

Red bars: The tester received a 802.11d country code from the access point. The country is different from the country selected in **Tools** > **Set country** in the tester.

n40+ n40–: Access points that use the 802.11n standard can bond a channel with an extension channel above (n40+) or below it (n40–) to make one 40 MHz channel. This wider channel gives the network higher throughput.

(...): All access points do not use the same 802.11 standard.

⑨ **Notes**: Press › to scroll to the notes field. The tester adds notes automatically. See page 35. Access points that have notes are purple.

(...): The access point has multiple notes. To see all notes, go to the **Access Point Details** screen.

⑩ : **Sort 1**, descending and ascending sequences

▼ ▲ : **Sort 2**, descending and ascending sequences

To sort the list in ascending or descending sequence, use ◁ and ◁ ▷ to highlight a column heading, then press SELECT or F1 **Sort 1**. For example, to quickly find the access point that has the strongest signal, highlight ▁▃▅▇ at the top of the column, then press SELECT or F1 **Sort 1**. This puts the access point with the strongest signal at the top of the list.

To sort in a secondary sequence, highlight a different column heading, then press F2 **Sort 2**.

⑪ Press F1 **Connect** to connect to the highlighted access point. See page 42.

The connect button shows as "**Connect***" if the tester cannot connect to the highlighted access point. See page 42.

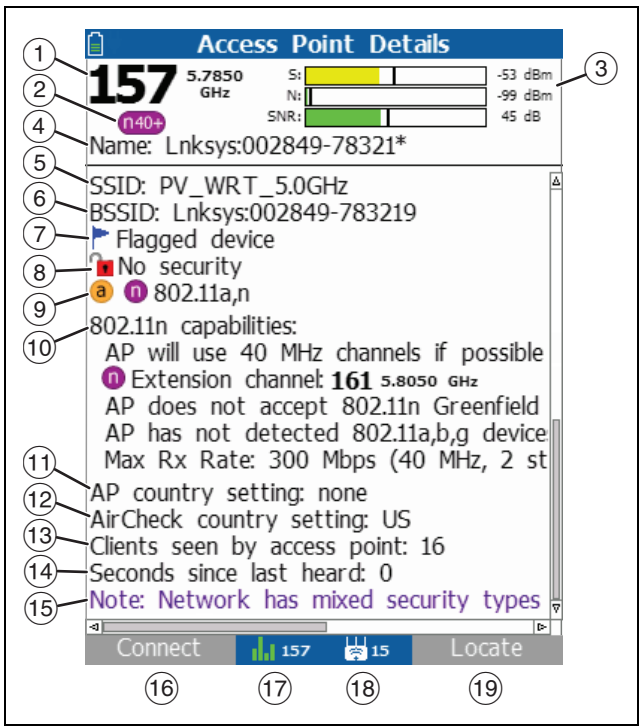
To connect to a secure access point, the tester must have a profile that includes security credentials. See page 14.

⑫ 48: The channel that the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20

⑬ 5: The number of access points that the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected. See page 18.

⑭ Press F2 **ACL** to change the authorization status for the highlighted access point. See page 17.

To see details for an access point, highlight the access point, then press SELECT. See Figure 7.



ffy06.eps

Figure 7. Access Point Details Screen

(1) The channel and frequency of the access point. The number is red if the channel is illegal for the country selected in **Tools** > **Set country**.

(2) n40+ n40–: The primary channel ((1)) is bonded with an extension channel above (n40+) or below it (n40–) to make one 40 MHz channel. This wider channel gives the network higher throughput. The extension channel shows under **802.11n capabilities** ((10)).

(3) The signal strength (**S**), noise strength (**N**), and signal to noise ratio (**SNR**). You can change the thresholds for the colors in the bar graphs. The bars are gray if the tester cannot hear the access point. See page 21.

(4) **Name**: The name of the access point, if a name is included in the beacon frames and probe response frames.

(5) **SSID**: Service Set Identifier. The name of the network that uses the access points.

(6) **BSSID**: Basic Service Set Identifier. The MAC address of the access point.

Note

Some access points have different MAC addresses for their wired and wireless interfaces.

(7) The authorization status for the access point.

⑧ The security status of the access point.

⑨ The 802.11 standards that the access point can use.

⑩ **802.11n capabilities**: Notes for access points that can use the 802.11n standard. See Table 4 on page 36.

⑪ **AP country setting**: The country code that the access point transmits. If the **AP country setting** does not agree with the **AirCheck country setting**, the access point has red bars in the **802.11** column. See "802.11d Operation" on page 20. Appendix C shows the countries for the codes.

⑫ **AirCheck country setting**: The code for the country selected in **Tools** > **Set country**. See "802.11d Operation" on page 20. Appendix C shows the countries for the codes.

⑬ **Clients seen by access point**: The number of clients that currently use the access point. "--" shows if the access point does not report the number of clients it has.

⑭ **Seconds since last heard**: The number of seconds since the tester heard the access point.

⑮ Notes for the access point. See Table 3 on page 35.

⑯ Press F1 **Connect** to connect to the access point. See page 42.

The connect button shows as "**Connect***" if the tester cannot connect to the highlighted network. See page 42.

⑰ : The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20

⑱ : The number of access points the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected. See page 17.

⑲ Press F2 **Locate** to locate the access point. See page 54.

If the Tester Does Not Discover an Access Point

In some situations, the tester will not discover an access point:

- The tester cannot hear the access point because you are too far away.
- The access point does not beacon when the tester listens to the channel that the access point uses.
- The tester cannot hear the access point because the signal cannot go through a wall or some other barrier.
- There is too much interference on the channel that the access point uses. Select **Channels** to see the interference from non-802.11 sources on the channel.

Notes for Networks and Access Points

Tables 3 and 4 give descriptions for the notes that the tester can add to networks and access points.

Table 3. Notes for Networks and Access Points

Ad hoc network operating	This SSID is an ad hoc network. A laptop broadcasts the SSID because the laptop automatically connected to a different laptop that transmitted the SSID. Ad hoc devices can give hackers access to data transmitted on the network. (Some IT policies for networks allow ad hoc devices.)
Channel is not legal for this country	The access point uses a channel that is not legal in the country selected in **Tools** > **Set country**. Make sure that the country selected in **Tools** > **Set country** is correct.
Possible Interference - overlaps standard channels	The access point uses a channel in the 2.4 GHz band that can have overlap with adjacent channels. This can cause interference on the adjacent channels. *Note* *In the United States, the channels that do not have overlap with each other are 1, 6, and 11.*

-continued-

Table 3. Notes for Networks and Access Points (continued)

Network has mixed security types	All access points for this SSID do not use the same type of security.
40 MHz 802.11n is not recommended on 2.4 GHz	You should not bond channels in the 2.4 GHz band because that band has only three channels that have no overlap with each other. If you bond two channels, then only one channel is available for other devices to use.
Unexpected country from access point	The country code from the access point does not agree with the country selected in **Tools** > **Set country** in the tester.

Table 4. 802.11n Capabilities (shown on the Access Points Details screen)

AP will use 40 MHz channels if possible	In some situations, the access point will not use 40 MHz channels. Examples: • The access point has heard other access points or clients that use channels that have overlap with 40 MHz channels. • A client that uses the access point has heard such access points or clients and told the access point not to use 40 MHz channels. See the 802.11n standard for all the situations where access points will not use 40 MHz channels.
AP is set to use only 20 MHz channels	The user has set the access point to use only 20 MHz channels.

Table 4. 802.11n Capabilities (shown on the Access Points Details screen) (continued)

AP accepts 802.11n Greenfield packets	The access point can increase speed if it uses Greenfield packets.
AP does not accept 802.11n Greenfield packets	The access point will not accept 802.11n Greenfield packets. The user has set the access point to never use Greenfield packets or the access point hears a, b, or g clients and will not operate Greenfield 802.11n mode.
AP has detected 802.11a, b, g devices	The access point must use protection so that it does not cause problems with a, b, or g transmissions. Protection procedures decrease the speed of the 802.11n network. • The access point has heard 802.11a, b, or g access points or clients. • A client that uses the access point has heard 802.11a, b, or g access points or clients.
AP has not detected 802.11a, b, g devices	It is not necessary for the access point to use protection to prevent problems with a, b, or g transmissions. The access point can operate at maximum speed.

-continued-

Table 4. 802.11n Capabilities (shown on the Access Points Details screen) (continued)

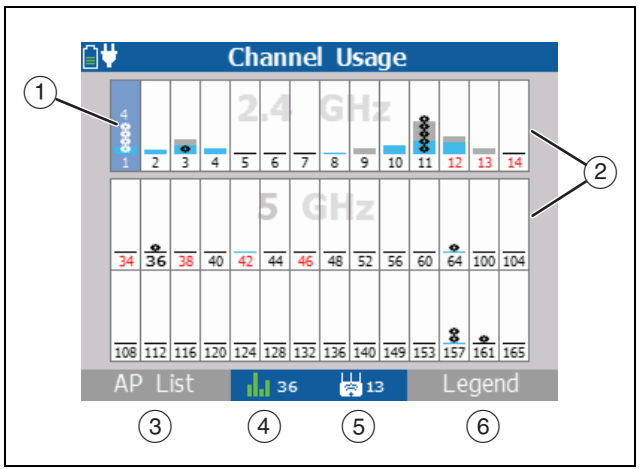
Max Rx Rate	The maximum rate of data reception for the access point at this time. The rate can change as the access point adjusts for changes in wireless traffic in the area. • **20 MHz** or **40 MHz**: The width of the channel that is necessary to get the maximum rate. • **X streams**: The number of data streams that the access point uses to get the maximum rate. • **1/2 GI**: The access point uses a short guard interval (400 ns instead of 800 ns) to get the maximum rate. For example, a short guard interval can increase the rate of reception from 270 Mbps to 300 Mbps.

Channel Usage

The channel usage function shows you how much wireless traffic is on each channel. It also shows interference from non-802.11 sources. Figure 8 shows the **Channel Usage** screen.

To see details for a channel (Figure 9), use to highlight a channel, then press

To select the bands for this function, select **Tools**, then select **Manage 802.11 settings**. See Table 2 on page 17.



ffy08.eps

Figure 8. Channel Usage Screen

(1) The bar graphs show how much of the channel capacity is used by 802.11 devices (blue) and by non-802.11 devices (gray). The taller the bar, the busier the channel.

The rings in the bar graphs show how many access points use the channel. When you highlight the channel, the number of active access points shows above the bar graph.

Channels that do not have access points can show 802.11 usage because of overlap from access points on adjacent channels.

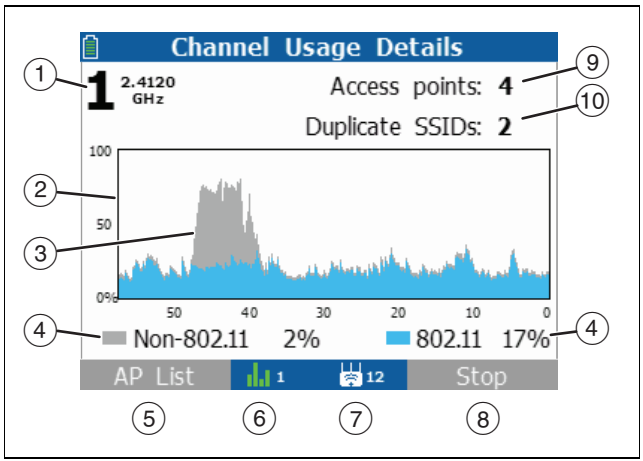
(2) By default, the tester shows channels on the 2.4 GHz and 5 GHz bands. To see only one band, change the setting in **Tools** > **Manage 802.11 settings**.

(3) Press F1 **AP List** to see the access points that use the highlighted channel.

(4) 48: The channel that the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20

(5) 5: The number of access points that the tester hears at your location. This shows the number of physical access points if **Group virtual access points** is selected. See page 17.

(6) To see descriptions of the icons on the **Channel Usage** screen, press F2 **Legend**.



ffy09.eps

Figure 9. Channel Usage Details Screen

1. The channel number and frequency of the channel that is monitored. The number is red if the channel is illegal for the country selected in **Tools** > **Set country**.

   To change the channel, press ◄►▲▼.

2. A graph of the 802.11 usage and non-802.11 interference of the selected channel over time in seconds.The more the usage, the busier the channel. Very busy channels can make the network slow or affect connectivity

3. Interference from a microwave oven.

4. **Non-802.11**, **802.11**: The percentage of signals on the channel that are not from 802.11 devices (gray) and that are from 802.11 devices (blue).

   Non-802.11 noise can come from microwave ovens, wireless telephones, Bluetooth® devices, motion detectors, wireless cameras and other wireless devices. This noise can interfere with WLAN connections or performance.

5. Press F1 **AP List** to see the access points that use the channel. See Figure 6.

6. 48: The channel that the access point uses. The color of the bars shows the status of the country code for the regulatory domain. The bars are red if the tester has received different country codes from two or more access points. See “802.11d Operation” on page 20.

⑦ : The number of access points the tester hears at your location. This shows the number of physical access points if **Group virtual access points** is selected. See page 18.

⑧ Press F2 **Stop** to stop the screen.

⑨ **Access Points**: The number of access points that use the channel. This shows the number of physical access points if **Group virtual access points** is selected. See page 18.

⑩ **Duplicate SSIDs**: The number of access points in the same area that use the same channel and support the same network. This can be a problem because the access points can interfere with each other.

Verify Connectivity

Use connectivity tests to verify the operation of these wireless network functions:

- Clients can connect to the network.
- Clients have access to network services (for example, DHCP, DNS, and routers).
- Clients can communicate with other devices in a reasonable amount of time.
- The range for client connections is satisfactory.

The tests also measure performance parameters that can show you if the network has a problem.

Load a Profile that Includes Security Credentials

The tester must have the correct security credentials to connect to a secure network. Secure networks have a green or yellow closed lock ( ) in the security column.

To enter security credentials, use AirCheck Manager to make a configuration profile that includes the credentials. Then, transfer the profile to the tester. See page 14.

Note

You cannot make or edit security credentials on the tester. You can make or edit them only with AirCheck Manager.

To load a profile

1 From the home screen, select **Tools**, then select **Manage files**.

2 Select **Load profile**, highlight the correct profile, press SELECT, then press F2 **Load**.

Connect to a Network or Access Point

The tester can connect to a network (SSID) or to a specified access point (BSSID) to make sure that the network or access point is available to wireless clients.

You can also use the tester to connect to a secure network to verify that security credentials are correct.

The tester shows the steps in the connection procedure, and gives a log of events that occur (Figures 10 and 11).

The connect button shows as "**Connect***" if the tester cannot connect to the highlighted network or access point. This occurs because the network uses security credentials that are not included in the profile that is loaded.

To connect to a network

1. If the network is secure, you must load a configuration profile that has security credentials for the network. See page 14.
2. From the home screen, select **Networks**.
3. Highlight the network in the **Networks (SSIDs)** list, then press F1 **Connect**.

To connect to a specified access point

1. If the access point is secure, you must use a configuration profile that has security credentials for the access point. See page 14.
2. From the home screen, select **Access Points**.
3. Highlight the access point in the **Access Points** list, then press F1 **Connect**.

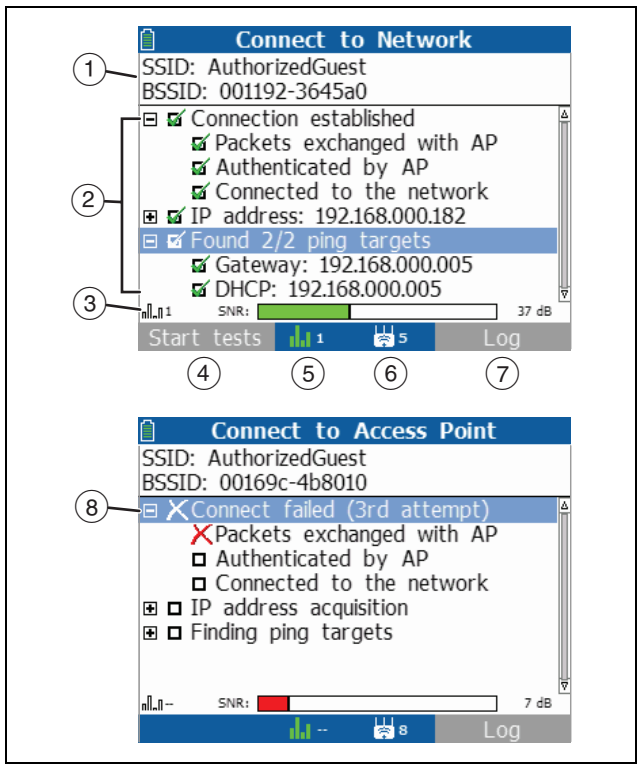


Figure 10. The Connection Screen

1. **SSID**, **BSSID**: The name of the network and the MAC address of the access point that the tester uses for the connection. When you connect to a network, the tester usually connects through the access point that has the highest signal to noise ratio. If the network includes secure and unsecure access points and security credentials are available, the tester tries to connect to the secure access point that has the highest signal to noise ratio. Some networks use a controller that connects you to the access point that has the least amount of traffic.

2. The steps in the connection procedure. The list for each step collapses when the step is completed. To expand or collapse the list for a step, highlight the step then press SELECT.

   As part of the connection test, the tester pings devices that support the connection (for example, the DHCP and DNS servers) and IP addresses that are included in the profile. The tester shows a green checkmark (☑)if the device responded or a red X (☒) if it did not respond. To ping other devices, do a ping test. See page 46.

3. **SNR**: The channel number and signal to noise ratio for the access point. You can change the thresholds for the colors in the bar graphs. See page 21.

④ Press F1 **Start tests** to do a ping test, which includes the **Connection range** test

⑤ 48: The channel that the access point uses. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20.

⑥ 5: The number of access points that the tester hears at your location. This shows the number of physical access points if **Group virtual access points** is selected. See page 18.

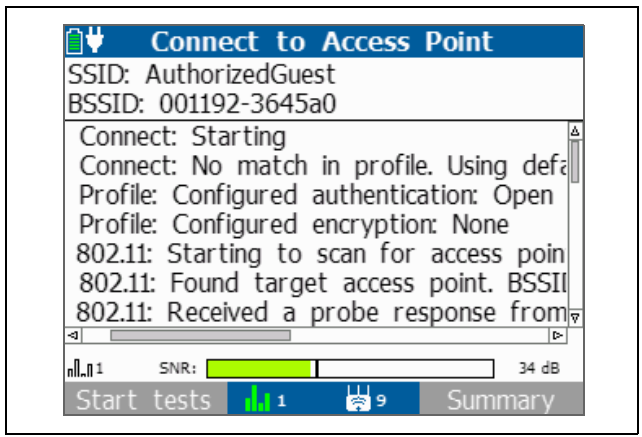
⑦ Press F2 **Log** to see details about the connection procedure. See Figure 11.

⑧ A connection that failed. The tester stops the connection process after the third attempt.

Appendix A describes log messages that show when the connection fails.

Note

On the connection log screen, press ◂ to scroll to see the timestamps for each entry in the log. The timestamps are in seconds.



ffy10.bmp

Figure 11. The Connection Log

Ping a Device or Web Server

You can enter addresses to ping other devices or web servers. This makes sure that other network devices are accessible and measures the response time.

1 Connect to a network or access point. See page 42.

2 When the connection is completed, press F1 **Start tests**.

Select an IP address from the list or enter a new address.

To enter a new address

a. Select **Enter IP address**.

b. Use ◀ ▶ to select a value to change.

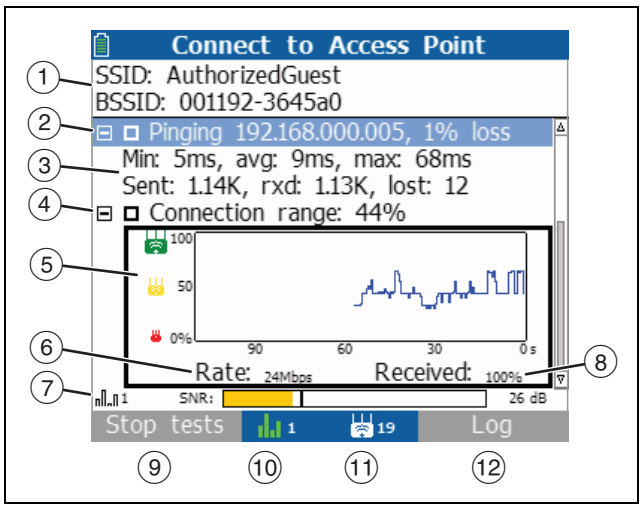
c. Use ▼ ▲ to increase or decrease the highlighted value.

d. To save the address, press F2 **Done**.

Note

If you save the profile, the tester does not save the ping addresses you enter. To include the addresses in the IP address list for ping tests, use AirCheck Manager to include them in a profile.

The ping screen (Figure 12) shows the results of the ping test. To ping a different address, press F1 twice, then select or enter a different address.



ffy21.eps

Figure 12. The Ping Screen

1. **SSID**, **BSSID**: Network name and access point name for the ping target.
2. **Pinging**: IP address for the ping target and the percentage of responses not received.
3. The minimum (**Min**), average (**avg**), and maximum (**max**) periods of time for ping responses from the device and the number of packets sent, received, and lost during the ping test.
4. **Connection range**: The connection range shows the probability of the best possible connection to the access point from your location. The best possible connection gives a ping response rate of 100% and the maximum possible data rate. The connection range value decreases as you move farther away from the access point. First, the data rate decreases. As you continue to move away from the access point, the ping response rate decreases and the connection becomes unreliable.

   The tester uses this formula to calculate the connection range:

$$\text{ping response rate (8)} \times \left(\frac{\text{data rate (6)}}{\text{maximum possible data rate}} \right)$$

5. A graph of the connection range for the last 120 seconds.
6. **Rate**: The data transfer rate.

⑦ **SNR**: The channel number of the access point and the signal to noise ratio. You can change the thresholds for the colors in the bar graph. See page 21.

⑧ **Received**: The ping response rate (pings responses received divided by pings sent).

⑨ Press F1 **Stop tests** to stop the ping test.

⑩ 48: The channel that the access point uses. The color of the bars shows the status of the country code for the regulatory domain. See “802.11d Operation” on page 20

⑪ 5: The number of access points that the tester hears at your location. This shows the number of physical access points if **Group virtual access points** is selected. See page 18.

⑫ Press F2 **Log** to see details about the connection procedure. See Figure 11.

Discover Clients

When the tester is on, it monitors each channel for probe request frames from network clients. To see these clients, use the **List clients** function. This function shows you if the network interface card in a client can transmit data. It also shows you information about the client, such as the channels it uses, its data rates, and the SSIDs it uses in probes.

The client screens include a **Locate** function that helps you find clients.

When you use the **List clients** function, the tester monitors each channel for a longer time than when you use other functions. This lets the tester find more clients on each channel.

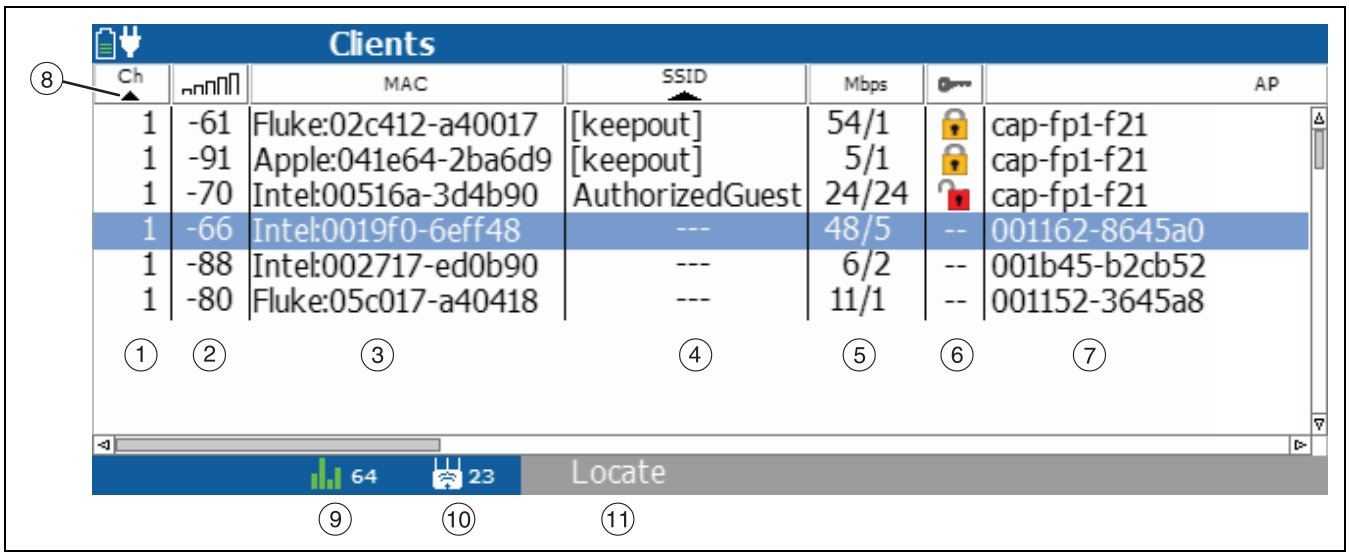
To discover clients

Select **Tools**, then select **List clients**. Figure 13 shows the **Clients** screen.

To see details about a client, highlight the client, then press SELECT. See Figure 14.

Note

The tester shows the most recent information for a client only when the client transmits data while the tester monitors the channel that the client uses. To collect client information more quickly, go to ***Tools*** *>* ***Manage 802.11 settings*** *and enable only one band. This decreases the number of channels that the tester monitors.*



ffy12.eps

Figure 13. Clients Screen

① **Ch**: The channel that the client uses.

② : The strength of the signal. You can change the thresholds for the colors in the bar graphs. See page 21.

③ **MAC**: The MAC address of the client. The address starts with a vendor abbreviation prefix, if the prefix is available. See “oui_abbr.txt” on page 64.

④ **SSID**: Service Set Identifier. The client is connected to this network.

[Hidden]: The network does not broadcast its SSID.

If an SSID shows in square brackets, the tester found the hidden SSID in packets from other wireless clients. In AirCheck Manager, these SSIDs show without square brackets.

⑤ **Mbps**: The maximum and minimum rates of data transfer that the tester saw the last time it monitored the client.

⑥ : The security status of the access point:

Red open lock: The access point does not have security enabled.

Yellow closed lock: The access point uses WEP security protocol.

Green closed lock: The access point uses a security protocol that is more secure than WEP, for example, WPA or WPA2.

⑦ **AP**: The name or BSSID of the access point that the client uses for the network connection.

⑧ : **Sort 1**, descending and ascending sequences

: **Sort 2**, descending and ascending sequences

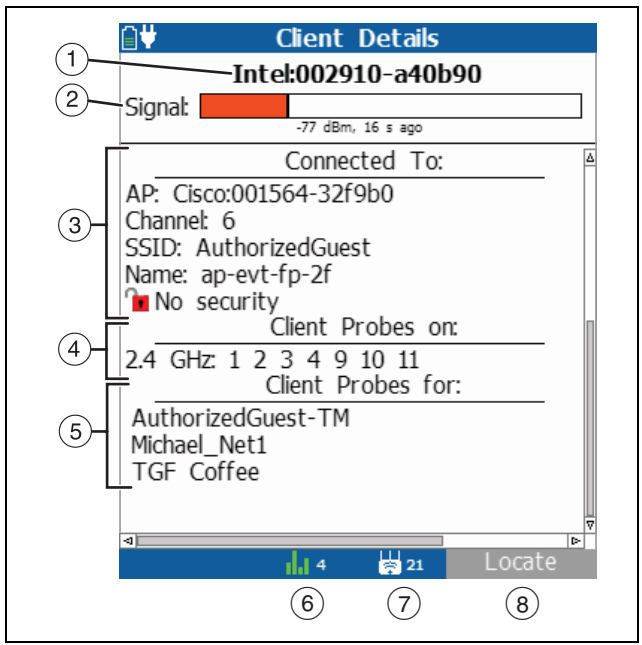
To sort the list in ascending or descending sequence, use and to highlight a column heading, then press or F1 **Sort 1**. For example, to quickly find the access point that has the strongest signal, highlight at the top of the column, then press or F1 **Sort 1**. This puts the access point with the strongest signal at the top of the list.

To sort in a secondary sequence, highlight a different column heading, then press F2 **Sort 2**.

⑨ 48: The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See “802.11d Operation” on page 20

⑩ 5: The number of access points the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected. See page 18.

⑪ Press F2 **Locate** to locate the client. See page 54.



ffy11.eps

Figure 14. Client Details Screen

1. The MAC address of the client. The address starts with a vendor abbreviation prefix, if the prefix is available. See "oui_abbr.txt" on page 64.
2. **Signal**: The signal strength of the last transmission from the client and the time since the tester heard the transmission. After 120 seconds, the units change to minutes. After 120 minutes, the units change to hours.
3. **Connected to**: If the client is or was connected to a network or recently tried to connect, this section shows information about the access point that the client used. If this section shows only the BSSID and channel for the access point, the tester needs more time to collect information.
4. **Client probes on**: The channels that the client probes.
5. **Client probes for**: SSIDs the client uses for probes. When a client connects to a network, it sometimes does not probe for other networks, so the list does not always show all the SSIDs the client can use. More SSIDs will show if the client roams.
6. : The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20
7. : The number of access points the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected. See page 18.
8. Press F2 **Locate** to locate the client. See page 54.

If the Tester Does Not Discover a Client

In some situations, the tester will not discover a client:

- The wireless card in the client is disabled.
- The tester cannot hear the client because you are too far away from the client.
- The tester cannot hear the client because the signal cannot go through a wall or some other barrier.
- There is too much interference on the channel that the client uses. Select **Channels** to see the interference from non-802.11 sources on the channel.
- The tester does not scan the band that the client uses. See the setting in **Tools** > **Manage 802.11 settings**.
- The client does not transmit a probe when the tester listens to the channel that the client uses.

Locate an Access Point or a Client

1 To locate an access point: Select **Networks** or **Access Points**, then use ◁▽△▷ and SELECT to go to the **Access Point Details** screen for the access point you want to locate.

To locate a client: Select **Tools**, then select **List clients**. Use ◁▽△▷ to highlight the client you want to locate.

2 Press F2 **Locate**. Figure 15 shows the **Locate Access Point** screen. Figure 16 shows the **Locate Client** screen.

3 Divide the area you want to search into four sections, as shown in Figure 17. Go to one corner of the area.

4 Make a note of the signal strength.

5 Go to the other three corners of the area and make a note of the signal strength at each corner.

6 Go to the first corner of the section that has the strongest signal.

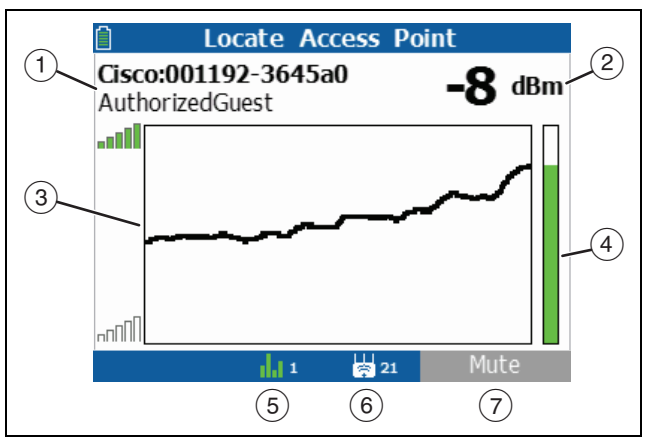
7 Do steps 4, 5, and 6 again until you find the access point or client.

Notes

If you do not find the access point or client, look on the floor above or below you.

If you cannot find a client, and the client shows a connection to the network, first find the access point that the client used, then look for the client.

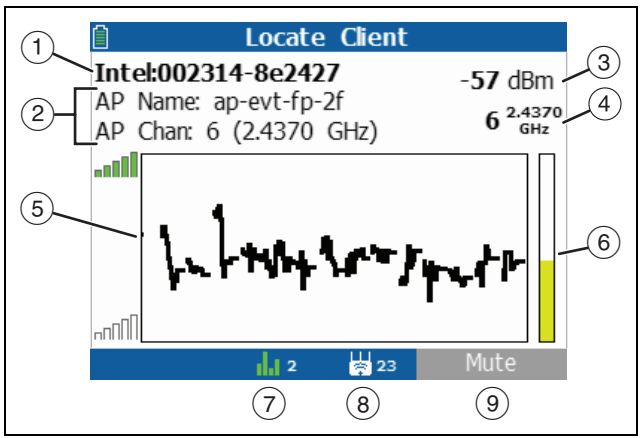
In large, open areas the optional external antenna can help you locate access points or clients more quickly. See page 58.



ffy07.eps

Figure 15. Locate Access Point Screen

1. Network name (SSID) and access point MAC address (BSSID).
2. The strength of the signal from the access point. The display shows "**---**" if the tester cannot hear the access point.
3. A graph of the signal strength over time. If the tester cannot hear the access point, the line does not show.
4. A gauge that shows the signal strength at the current time. The bar is gray if the tester cannot hear the access point.
5. 48: The channel that the access point uses. The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20
6. 5: The number of access points that the tester has found. This number does not include virtual access points if **Group virtual access points** is selected. See page 17.
7. Press F2 **Mute** to turn off the sound.



ffy18.eps

Figure 16. Locate Client Screen

(1) The MAC address of the client. The address starts with a vendor abbreviation prefix, if the prefix is available. See "oui_abbr.txt" on page 64.

(2) The name, channel, and frequency of the access point that the client uses for the network connection.

(3) The strength of the signal from the client. The display shows "**---**" if the tester cannot hear the client.

(4) The channel that the tester monitors the most. This is the channel that the client used the last time the tester heard the client. The tester monitors this channel for 2 seconds, monitors another channel for 1 second, then monitors the first channel again for 2 seconds. If the client changes its channel, the tester will find the client on the new channel after some time.

To change this channel, press ◀ ▶. The tester monitors the new channel for 2 seconds, and continues to monitor the other channels as before.

(5) A graph of the signal strength over time. If the tester cannot hear the client, the line does not show.

(6) A gauge that shows the signal strength at the current time. The bar is gray if the tester cannot hear the client.

(7) 48: The channel that the tester monitors. See (4).

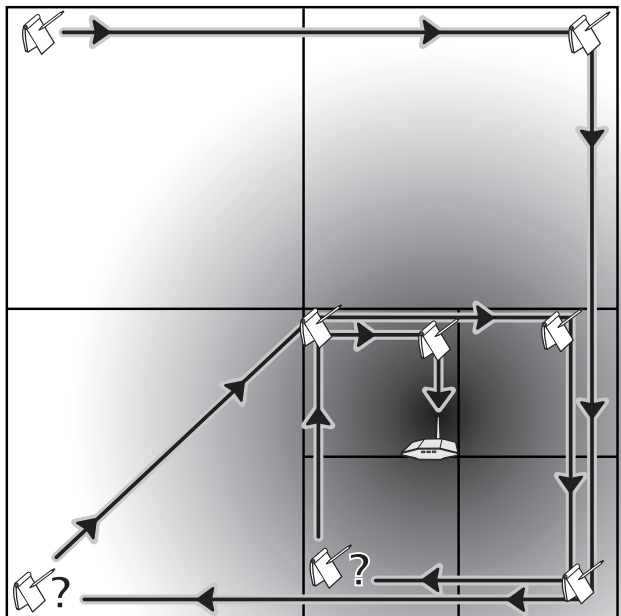
The color of the bars shows the status of the country code for the regulatory domain. See "802.11d Operation" on page 20

(8) 5: The number of access points that the tester has found. This number does not include virtual access points if **Group virtual access points** is selected. See page 17.

(9) Press F2 **Mute** to turn off the sound.

Make a note of the signal strength.

? Go to the first corner of the section that had the strongest signal.



ffy16.eps

Figure 17. Search Pattern for the Omnidirectional Antenna in the Tester

The External Directional Antenna

In large, open areas, the external directional antenna can show you the direction of a signal source more precisely than the omnidirectional antenna in the tester.

Note

In areas that have many rooms, for example in schools and hospitals, use the internal omnidirectional antenna to locate access points.

To use the external antenna

1 Connect the antenna to the antenna jack on the rear of the tester. The screen shows the antenna icon ( ) when you connect the antenna. The tester uses only the external antenna when the antenna is connected.

Note

When the external antenna is connected, the tester will not transmit, so it will not connect to a network or access point.

2 Divide the area into four sections, as shown in Figure 18. Go to the center of the area.

3 To locate an access point: Select **Networks** or **Access Points**, then use ◄► and SELECT to go to the **Access Point Details** screen for the access point you want to locate.

To locate a client: Select **Tools**, then select **List clients**. Use ▲▼ to highlight the client you want to locate.

4 Press F2 **Locate**.

5 Point the antenna to each corner of the area. Figure 19 shows how to point the antenna.

6 Go to the middle of the section that has the strongest signal.

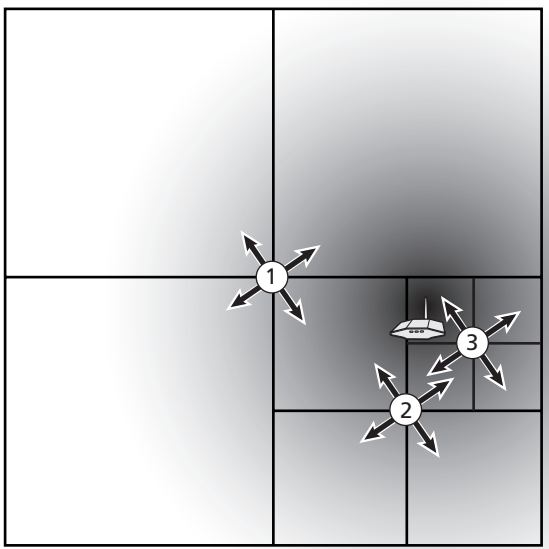
7 Repeat steps 2, 5, and 6 until you find the access point or client.

Note

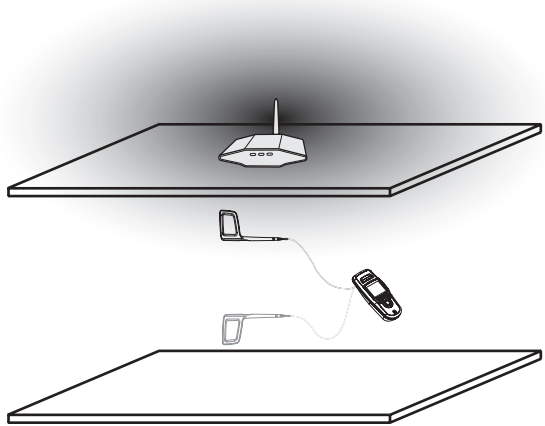
If you do not find the access point or client, look on the floor above or below you.

Use these guidelines when you use the external antenna:

- Hold the antenna at a constant height. You can get more stable measurements if you hold the antenna above cubicle walls.
- When you point the antenna in different directions, do not move your arm. Hold the tester and antenna in one position while you turn your body.



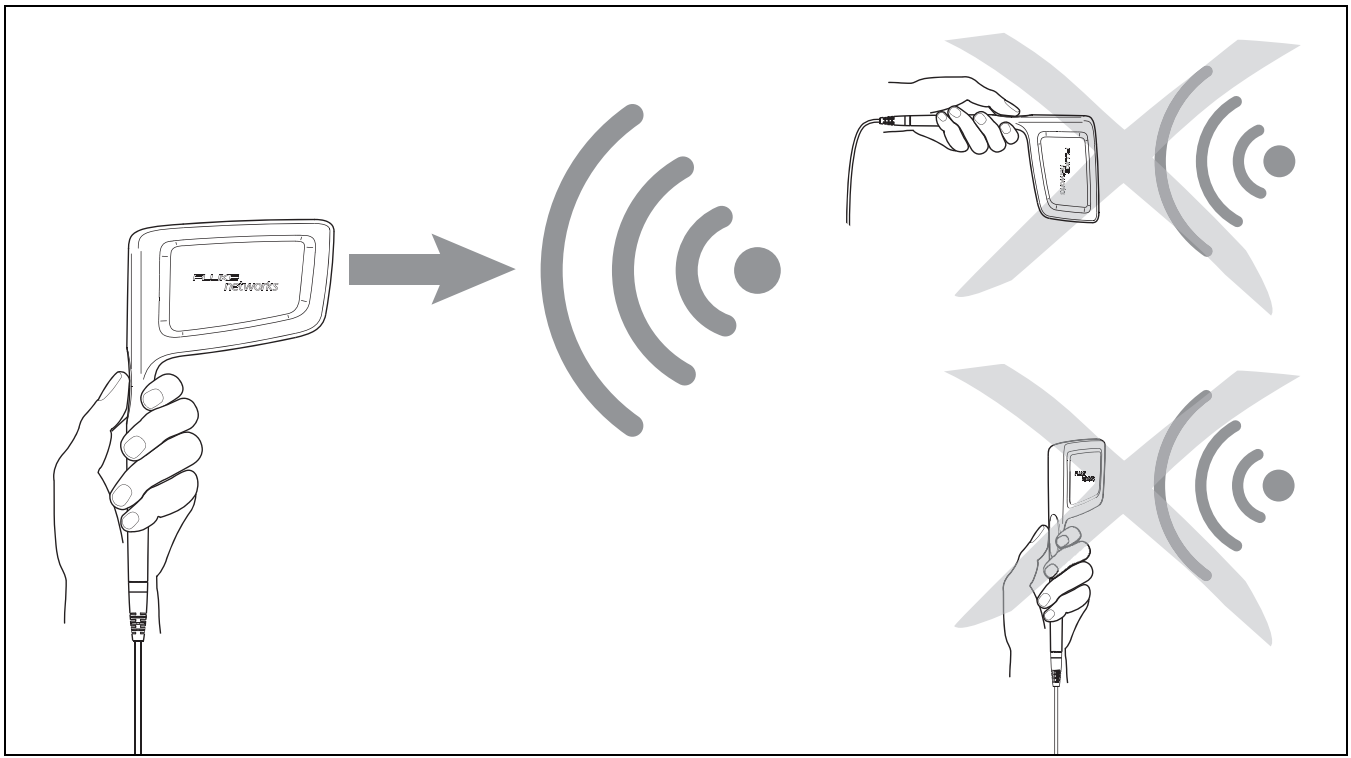
Go to the middle of the section that has the strongest signal until you find the access point.



The signal can be stronger above or below you.

ffy17.eps

Figure 18. Search Pattern for the External Antenna



ffy13.eps

Figure 19. How to Point the External Antenna

Adjust Signal Strength Measurements to Agree with Other Devices

Signal strength measurements from different models of wireless testers or from clients used as a reference do not always agree with each other. The differences are caused mainly by differences in the antennas. To make the devices agree, you can add an offset to the AirCheck measurements.

To add an offset to signal strength measurements

1 Find the offset value:

Use the AirCheck tester and the other device to measure the signal strength in the same location. Record the difference in the measurement for each channel that is important to you.

2 Select **Tools**.

3 Select **Manage 802.11 settings**, then select **Use custom signal adjustment**.

4 On the **User Offsets** screen, use ↕ to select a channel, then use ↔ to select an offset value.

5 Repeat step 4 as necessary for other channels.

6 To save the offset values, press F2 **Save**.

When you turn off the tester, it saves the offsets in the profile. The offsets also show in reports you make with AirCheck Manager.

⚠ Caution

To prevent inconsistent measurements later, be sure to remember that you adjusted the offsets.

Save a Test Session

You can save the information the tester has collected since you turned it on or since the last time you saved a session, pressed , or disconnected the USB cable. A session includes this information:

- Network, access point, client, and channel information (does not include graphs)
- A list of clients that transmitted probes
- Results for the last connection you made
- Results for the last ping test you did
- The connection log

To save the data from a test session

1 Press . The tester shows a default, sequential filename at the bottom of the screen.

- To save the session with the filename shown, press F2 **Save**. The tester saves the session in the "SESSIONS" folder.
- To overwrite a test session that is saved on the tester, highlight the test session, press SELECT, press F2 **Save**, then press F2 **OK**.
- To edit the filename, press F1 **Edit**.

Note

Session names can have a maximum of 8 characters with an extension of 3 characters. The extension must be ".ACS" if you want to see the session in AirCheck Manager.

- To delete characters in the filename, press F1 **Delete**.
- To add characters to the filename, use ◀ ▶ to highlight a character, then press SELECT.
- To move the cursor in the filename, highlight the filename, then press ◀ ▶.
- To save the session with the edited filename, press F2 **Done**, then press F2 **Save**.

To see the session file, open it in AirCheck Manager. See page 65.

Manage Files on the Tester

To rename a file

1 Select **Tools**, then select **Manage files**.

2 Select **Rename file**.

3 Highlight a file, then press SELECT.

4 To edit the filename, press F1 **Edit**.

Note

Sessions must have the extension ".ACS" and profiles must have the extension ".ACP" if you want to see them in AirCheck Manager.

- To delete characters in the filename, press F1 **Delete**.
- To add characters to the filename, use ▲▼◀▶ to highlight a character, then press SELECT.
- To move the cursor in the filename, highlight the filename, then press ◀▶.

5 To rename the file with the name you made, press F2 **Done**, then press F2 **Rename**.

To delete a file

1 Select **Tools**, then select **Manage files**.

2 Select **Delete file**.

3 Highlight a file, then press SELECT.

4 Press F2 **Delete**.

Note

If you delete or rename a file that the tester must have to operate the tester will recreate the file the next time you turn on the tester. This does not occur for profiles you created, session files you saved, or for the file OUI_ABBR.TXT. See "About Files on the Tester" on page 64.

To see how much space is available in memory

Use the USB cable supplied with the tester to connect the tester to the PC, then use one of these procedures:

- Start AirCheck Manager, select **Tools** > **Profile Manager**, then look at the **Memory Used** graph.
- Use the file browser in the PC operating system to see how much memory space is available on the tester.

If memory is full, the tester shows **Memory full** when you try to save a file.

About Files on the Tester

The tester saves data in XML (Extensible Markup Language) format. The data in XML files includes identification tags. Software that can read the tags can use the data. For example, a web browser that can read the tags can show XML files on a web page.

The tester makes these types of XML files (default filenames):

- DEVICE.XML: This file contains the information shown when you select **Tools** > **View AirCheck Information**.
- CURRENT.ACP: This file contains a copy of the current profile. It also contains changes you made to settings on the tester since you saved or loaded the profile.
- SNXXXXXX.ACS: Session files contain information about wireless networks. See "Locate an Access Point or a Client" on page 54. AirCheck Manager uses session files to create session reports.

The text file OUI_ABBR.TXT contains abbreviations for the names of manufacturers who make interface devices for networks. The tester uses the abbreviations as prefixes for MAC addresses.

To load the latest list of vendor prefixes into the tester

1. Start the latest version of AirCheck Manager on your PC, then connect the tester to the PC.
2. Select **AirCheck** > **Update Software**, then select the **Vendor MAC Prefix File** tab.
3. Click **Update from file**, select the prefix file (oui_abbr.txt), then click **Open**.

If there is a newer list on the Fluke Networks website that is not included in the latest version of AirCheck Manager, copy the file to the "VendorPrefix" folder for AirCheck Manager. Then, do the steps given above to load the list into the tester.

Transfer Files to a PC

To use AirCheck Manager to look at test sessions or profiles that are saved on the tester

1 Install the latest version of AirCheck Manager software on your PC. Start the software.

2 Turn on the tester.

3 Use the USB cable supplied with the tester to connect the tester to the PC. The AirCheck pane shows session files that are on the tester.

To see the profiles that are on the tester, select **Tools** > **Profile Manager** from the AirCheck Manager tool bar.

To use the PC operating system to transfer files

1 Turn on the tester.

2 Use the USB cable supplied with the tester to connect the tester to the PC. The PC operating system shows the tester as a disk drive.

3 Use the PC operating system to copy files from the tester to a disk drive on the PC.

Maintenance

⚠Warning⚠

To prevent possible fire, electrical shock, personal injury, or damage to the tester:

- **Do not open the case. You cannot repair or replace parts in the case.**
- **Use only replacement parts that are approved by Fluke Networks.**
- **If you replace parts that are not specified as replacement parts, the warranty will not apply to the product and you can make the product dangerous to use.**
- **Use only service centers that are approved by Fluke Networks.**

Clean the Tester

To clean the display, use lens cleaner and a soft, lint-free cloth. To clean the case, use a soft cloth that is moist with water or water and a weak soap.

⚠Caution

To prevent damage to the display or the case, do not use solvents or abrasive materials.

Update the Software in the Tester

1 Download the AirCheck update file from the Fluke Networks website, or contact Fluke Networks to get the update by other means. Save the file to your hard disk.

2 Get the latest version of AirCheck Manager from the Fluke Networks website.

3 Start AirCheck Manager on your PC.

4 Turn on the tester.

5 Use the USB cable supplied with the tester to connect the tester to the PC.

6 In AirCheck Manager, select **AirCheck** > **Update Software**.

7 Click **Select**, find and select the update file (.xlf extension), then click **Open**.

8 Click **Update**.

9 When the transfer is completed, disconnect the USB cable from the tester.

10 The screen on the tester is blank and the tester ticks while it installs the update file. When the update is completed, the home screen shows on the tester.

Note

The power key is disabled during a software update. If you remove the battery before the update completes, the update starts again when you turn on the tester.

Restore Factory Defaults

Appendix B gives a list of the default settings for the tester.

To restore factory defaults

1 From the home screen, select **Tools**, select **Restore factory defaults**, then press F2 **OK**.

2 To complete the process, press SELECT, then turn the tester on.

Device Information

To see information about the tester

From the home screen, select **Tools**; then select **View AirCheck information**.

- **Serial Number**: The serial number is also shown under the battery pack.
- **MAC Address**: Media Access Control address. The unique address of the tester.
- **SW Version**: The version of software in the tester.
- **USB Version**: The version of the USB driver in the tester.
- **Radio Version**: The version of the radio in the tester.

If the Tester Will Not Turn Off

If the tester will not turn off, hold down ⏻ for approximately 5 seconds.

If the tester still does not turn off, remove the battery pack and install it again.

Options and Accessories

Table 5 shows options and accessories available for the AirCheck Wi-Fi Tester.

For a complete list of options and accessories visit the Fluke Networks website at www.flukenetworks.com.

Table 5. Options and Accessories

Option or Accessory	Fluke Networks Model Number
External directional antenna with RSMA connector	EXTANT-RPSMA
Lithium ion battery pack for the AirCheck tester	WBP-LION
Power over Ethernet detector	POE-DETECTOR
Adapter/charger for connection to an automobile cigarette lighter	MS-Auto-Chg
AC adapter/charger, universal, 120-240 Vac	DTX-ACUN

Specifications

Environmental Specifications

Operating temperature and relative humidity	32°F to 113°F (0°C to +45°C) *Note* *The battery will not charge if the internal temperature of the tester is above 113°F (45°C).*
Operating relative humidity (% RH without condensation)	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)
Storage temperature	-4°F to 140°F (-20°C to +60°C)
Shock and vibration	Random, 2 g, 5 Hz-500 Hz (Class 2) 1 m drop test
Safety	EN 61010-1 2nd edition
Altitude	4,000 m; Storage: 12,000 m
EMC	FCC Part 15 Class A, EN 61326-1

Certifications and compliance	Conforms to relevant European Union directives
	N10140 Conforms to relevant Australian standards
	C SA US Listed by the Canadian Standards Association
	Conforms to FCC Rules, Parts 15.107, 15.109
	ANATEL 1572-10-5988 (01)07898941652029 Certified by the National Agency of Telecommunications (Anatel)

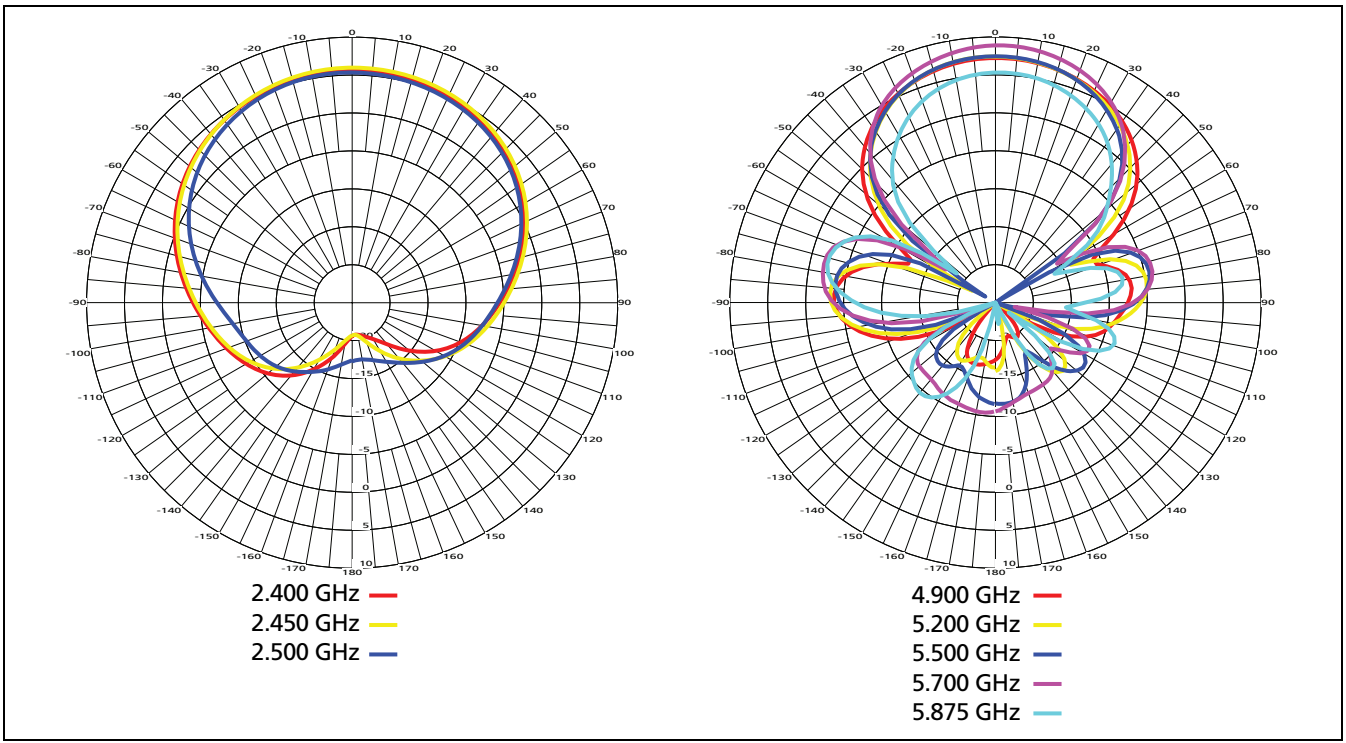
General Specifications

Dimensions	3.5 in x 7.8 in x 1.9 in (8.9 cm x 19.8 cm x 4.8 cm)
Weight	14 oz (0.4 kg)
Battery	Removable, rechargeable lithium-ion battery pack (18.5 Watt-hrs)
Battery life	Typical operating life is 5.5 hours. Typical charge time is 3 hours.
External AC adapter/charger	AC input 90-264 Vac 48-62 Hz input power DC output 15 Vdc at 1.2 amps
Display	2.8 in color LCD (320 x 240 pixels)
Keypad	12-key elastomeric
LEDs	2 LEDs (transmit and link Indicators)
Host interface	USB 5-pin mini-B
Wireless antenna	Internal
External antenna port	Input only. Reverse-polarity SMA connector.

Wireless Specifications

Specification compliance	IEEE 802.11a, 11b, 11g, 11n
Operating frequencies *Note* *These are the center frequencies of the channels that the AirCheck tester supports.*	**Frequencies of channels received** *Note* *The tester receives on all of the frequencies in every country.* 2.4 GHz band: 2.412 GHz to 2.484 GHz (channel 1 to channel 14) 5 GHz band: 5.170 GHz to 5.320 GHz, 5.500 GHz to 5.700 GHz, 5.745 GHz to 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165) **Frequencies of channels transmitted** *Note* *The tester transmits only on the frequencies allowed in the country where it is operating.* **2.4 GHz band** 802.11b: 2.412 GHz to 2.484 GHz (channel 1 to channel 14) 802.11 g/n 20 MHz BW (HT20): 2.412 GHz to 2.472 GHz (channel 1 to channel 13) 802.11 n 40 MHz BW (HT40): 2.422 GHz to 2.462 GHz (includes all combinations of legal, bonded pairs of channels)

	Frequencies of channels transmitted (continued) **5GHz band** 802.11 a /n 20 MHz BW (HT20): 5.180 GHz to 5.320 GHz, 5.500 GHz to 5.700 GHz, 5.745 GHz to 5.825 GHz (channels 36, 40, 44, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 1 36, 140, 149, 153, 157, 161, 165) 802.11 n 40 MHz BW (HT40): 5.190 GHz to 5.310 GHz, 5.510 GHz to 5.670 GHz, 5.755 GHz to 5.795 GHz (includes all combinations of legal, bonded pairs of channels)
Regulatory Domain	World Mode, 802.11d compliant
External Directional Antenna **Frequencies** **Connector**	 Frequency range 2.4 GHz to 2.5 GHz and 4.9 to 5.9 GHz Minimum gain 5.0 dBi in the 2.4 GHz band and 7.0 dBi in the 5 GHz band Reverse-polarity SMA plug



ffy20.eps

Figure 20. Antenna Patterns for the External Antenna (magnitude (dBi)) vs. azimuth (degrees)

Federal Communication Commission and Industry Canada Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC and IC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC and IC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Important Note: FCC and IC Radiation Exposure Statement

This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15 GHz to 5.25 GHz band are restricted to indoor usage only.

The availability of some specific channels and/or operational frequency bands are country dependent and not accessible by the end user.

Europe-EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1: 2001 A11: 2004**

  Safety of Information Technology Equipment

- **EN50385: (2002-08)**

  Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz to 40 GHz) -General public

- **EN 300328 V1.7.1: (2006-10)**

  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- **EN 301 893 V1.4.1: (2007-07)**

  Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

- **EN 301 489-1 V1.6.1: (2005-09)**

  Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- **EN 301 489-17 V1.2.1 (2002-08)**

  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 MHz to 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Appendix A: Log Messages for Connections that Fail

The connection log (page 45) can help you understand why a device cannot connect to a network. This appendix gives reasons for log messages that show when a connection fails.

Message	Possible Reasons for the Connection Failure
802.11: Found no access points	The access point is out of range, disabled, or someone changed the frequency band.
802.11: Warning: Found access point with SSID, but security configurations mismatch	The tester does not have the correct types of 802.1X authentication/ encryption.

Message	Possible Reasons for the Connection Failure
Authentication failed	The access control list and MAC filter on the access point rejected the MAC of the tester. The access point uses WEP security, and the low-level 802.11 authentication (open/shared) that the tester uses is different from the type of authentication that the access point uses.
802.11: Received deauthentication packet	When this follows the message **802.1X: Sending EAP 4-way key with client nonce and info elements**, it is frequently caused by an incorrect pre-shared key (passphrase).
Connect: Fail expected during automatic PAC provision (phase 0)	The tester always shows this message when it uses EAP-FAST authentication to try to connect to an access point. Multiple phases are necessary for an EAP-FAST connection, and there is usually a failure during the initial phase.
802.1X: Received EAP fail	• When this follows the message **802.1X TLS: Sending client key exchange**, it is frequently caused by an incorrect client certificate. • When this follows the message **802.1X EAP-MSCHAPv2: Responding to challenge**, it is frequently caused by an incorrect user name or password. • When this follows the message **802.1X: NAK**, it frequently occurs because the RADIUS server does not support the EAP type.

Message	Possible Reasons for the Connection Failure
802.1X: Server certificate unverified	Ignore this message if you did not select the option **Check Server Certificate** in the profile in AirCheck Manager.
802.1X: Server certificate is bad	The option **Check Server Certificate** was selected in the profile in AirCheck Manager, but an incorrect certificate was loaded into the tester.
DHCP: Timeout occurred (without the message **DHCP: Success** after this one)	• The access point could not communicate with the external DHCP server. • The access point has an internal DHCP server, but it is disabled. • The DHCP server is at its limit for the number of users. • The tester and the access point are both configured for WEP security, but they have different key settings.
DHCP: No offer received	When this follows the message **DHCP: Timeout occurred**, see the causes above.
Static IP: ARP received. Address already in use	The option **Manual (Static)** was selected in the profile in AirCheck Manager, but a duplicate IP address was found on the network.

Appendix B: Default Settings

This appendix shows the default settings for the tester when you select **Tools** > **Restore factory defaults**.

Function	Default Setting
Profile that the tester uses	Default
Auto shutoff	On
Language	The language that was selected last
Country	US
Sound for the AP Locate function	On

Function	Default Setting
Thresholds for Bar Graphs	
Signal Level: Red	-80 dBm
Signal Level: Yellow	-60 dBm
Signal Level: Green	-45 dBm
Noise Level: Red	-60 dBm
Noise Level: Yellow	-80 dBm
Noise Level: Green	-90 dBm
S/N Level: Red	20 dB
S/N Level: Yellow	30 dB
S/N Level: Green	40 dB

Function	Default Setting
802.11 Settings	
Bands	2.4 GHz and 5 GHz
Transmit probes	Enable
Group virtual access points	Enable
Gray inaudible access points or Delete inaudible access points	Gray inaudible access points
User offsets for custom signal adjustments	0 dB
Network (SSIDs) List	
Sort 1	SSID
Sort 2	SSID
Individual Networks	
Sort 1	Name/MAC
Sort 2	Name/MAC

Function	Default Setting
Access Points on a Channel	
Sort 1	Name/MAC
Sort 2	Name/MAC
Access Points List	
Sort 1	Name/MAC
Sort 2	Name/MAC
Virtual Access Points List	
Sort 1	SSID
Sort 2	SSID
Clients List	
Sort 1	MAC
Sort 2	Channel

Appendix C: 802.11d Country Codes

This appendix shows the countries for the country codes that the tester shows on the **Access Point Details** screen.

Countries shown in bold text are the countries you can select in **Tools** > **Set country**.

Note

The tester can show a third character in the country code. You can ignore that character when you look for the country code in the table below.

AD	Andorra
AE	**United Arab Emirates**
AF	Afghanistan
AG	Antigua and Barbuda
AI	Anguilla
AL	**Albania**
AM	**Armenia**
AN	**Netherlands Antilles**
AO	Angola
AQ	Antarctica
AR	**Argentina**

AS	American Samoa
AT	**Austria**
AU	**Australia**
AW	Aruba
AX	Aland
AZ	**Azerbaijan**
BA	**Bosnia and Herzegovina**
BB	Barbados
BD	**Bangladesh**
BE	**Belgium**
BF	Burkina Faso
BG	**Bulgaria**
BH	**Bahrain**
BI	Burundi
BJ	Benin
BL	Saint Barthelemy
BM	Bermuda

BN	**Brunei Darussalam**
BO	**Bolivia**
BR	**Brazil**
BS	Bahamas
BT	Bhutan
BU	Burma (transitional)
BV	Bouvet Island
BW	Botswana
BY	**Belarus**
BZ	**Belize**
CA	**Canada**
CC	Cocos Islands
CD	Congo, Democratic Republic of
CF	Central African Republic
CG	Congo
CH	**Switzerland**
CI	Cote d'Ivoire

CK	Cook Islands
CL	**Chile**
CM	Cameroon
CN	**China**
CO	**Colombia**
CR	**Costa Rica**
CS	**Serbia and Montenegro (transitional)**
CU	Cuba
CV	Cape Verde
CX	Christmas Island
CY	**Cyprus**
CZ	**Czech Republic**
DE	**Germany**
DJ	Djibouti
DK	**Denmark**
DM	Dominica
DO	**Dominican Republic**

DZ	**Algeria**
EC	**Ecuador**
EE	**Estonia**
EG	**Egypt**
EH	Western Sahara
ER	Eritrea
ES	**Spain**
ET	Ethiopia
EU	European Union
FI	**Finland**
FJ	Fiji
FK	Falkland Islands (Malvinas)
FM	Micronesia
FO	Faroe Islands
FR	**France**
FX	France, Metropolitan
GA	Gabon

GB	**United Kingdom**
GD	Grenada
GE	**Georgia**
GF	French Guiana
GG	Guernsey
GH	Ghana
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	**Greece**
GS	South Georgia
GT	**Guatemala**
GU	Guam
GW	Guinea-Bissau
GY	Guyana
HK	**Hong Kong**
HM	Heard and McDonald Islands
HN	**Honduras**
HR	**Croatia**
HT	Haiti
HU	**Hungary**
ID	**Indonesia**
IE	**Ireland**
II	International (Cisco only)
IL	**Israel**
IM	Isle of Man
IN	**India**
IO	British Indian Ocean
IQ	Iraq
IR	Iran
IS	**Iceland**

IT	**Italy**
JE	Jersey
JM	**Jamaica**
JO	**Jordan**
JP	**Japan**
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis
KP	Korea, D.P.R. (north)
KR	**Korea, Republic (south)**
KW	**Kuwait**
KY	Cayman Islands
KZ	**Kazakhstan**
LA	Lao

LB	**Lebanon**
LC	Saint Lucia
LI	**Liechtenstein**
LK	**Sri Lanka**
LR	Liberia
LS	Lesotho
LT	**Lithuania**
LU	**Luxembourg**
LV	**Latvia**
LY	Libyan Arab Jamahiriya
MA	**Morocco**
MC	**Monaco**
MD	Moldova, Republic of
ME	Montenegro
MF	Saint Martin
MG	Madagascar
MH	Marshall Islands

MK	**Macedonia**
ML	Mali
MM	Myanmar
MN	Mongolia
MO	**Macau**
MP	Northern Mariana Islands
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	**Malta**
MU	Mauritius
MV	Maldives
MW	Malawi
MX	**Mexico**
MY	**Malaysia**
MZ	Mozambique

NA	No country is selected (special situation for some access points)
NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	**Netherlands**
NO	**Norway**
NP	**Nepal**
NR	Nauru
NT	Neutral Zone (transitional)
NU	Niue
NZ	**New Zealand**
OM	**Oman**
PA	**Panama**
PE	**Peru**

PF	French Polynesia
PG	**Papua New Guinea**
PH	**Philippines**
PK	**Pakistan**
PL	**Poland**
PM	Saint Pierre and Miquelon
PN	Pitcairn
PR	**Puerto Rico**
PS	Palestinian Territory
PS	United States (public safety)
PT	**Portugal**
PW	Palau
PY	Paraguay
QA	**Qatar**
RE	Reunion
RO	**Romania**
RS	Serbia

RU	**Russian Federation**
RW	Rwanda
SA	**Saudi Arabia**
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	**Sweden**
SF	Finland (unofficial)
SG	**Singapore**
SH	Saint Helena
SI	**Slovenia**
SJ	Svalbard and Jan Mayen
SK	**Slovakia**
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia

SR	Suriname
ST	Sao Tome and Principe
SU	USSR (formerly)
SV	**El Salvador**
SY	Syrian Arab Republic
SZ	Swaziland
TC	Turks and Caicos Islands
TD	Chad
TF	French Southern Territories
TG	Togo
TH	**Thailand**
TJ	Tajikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkmenistan
TN	**Tunisia**
TO	Tonga

TP	East Timor (transitional)
TR	**Turkey**
TT	**Trinidad and Tobago**
TV	Tuvalu
TW	**Taiwan**
TZ	Tanzania
UA	**Ukraine**
UG	Uganda
UK	United Kingdom (unofficial)
UM	U.S. Minor Outlying Islands
US	**United States**
UY	**Uruguay**
UZ	**Uzbekistan**
VA	Vatican City (Holy See)
VC	Saint Vincent and the Grenadines
VE	**Venezuela**
VG	Virgin Islands, British

VI	Virgin Islands, U.S.
VN	**Viet Nam**
VU	Vanuatu
WF	Wallis and Futuna Is.
WS	Samoa
YE	**Yemen**
YT	Mayotte
YU	Yugoslavia (transitional)
ZA	**South Africa**
ZM	Zambia
ZR	Zaire (transitional)
ZW	**Zimbabwe**

Index

Symbols

(...)
    access points list
        802.11, 30
        ACL, 29
        notes, 30
        security, 30
    networks list
        802.11, 26
        ACL, 25
        notes, 26
        security, 25
*
    access point, 29
    Connect, 42
    profile name, 13, 14

Numbers

802.11 settings, 17
802.11d, 20
802.11n capabilities, 36

–A–

a, 26
Access Point Details, 32
access points
    802.11d country, 33
    ACL (authorization status), 22
    connect to an access point, 42
    details screen, 32
    list, 28
    locate an access point, 54, 58
    ping, 46
accessories
    optional, 67
    standard, 3
ACL, 22
ACP files, 64
ACS files, 64

ad hoc device
    access points list, 30
    networks list, 25, 29
    note, 35
AirCheck Manager
    overview, 1
    profile, 14
    transfer files to a PC, 65
    update the software in the tester, 66
antenna
    external, 58
    internal, 57
authorization status, 22
authorized device, 22
auto shutoff, 19

–B–

b, 26
bar graph colors, 21
battery, 6

–C–

certifications and compliance, 72
channels
    channel usage, 38
    channel usage details, 40
    default, 20
    frequency bands, 17
    interference
        note, 35
        on usage graph, 40
cleaning, 66
clients, 49
compliance statement, 75
connect to a network or access point, 42
connection range, 47
country, 19
    code from access points, 20
    codes, 85
    setting, 19
CURRENT.ACP, 64
custom signal adjustment, 61
customer support, 2

–D–

date, 19
default settings, 83
Delete inaudible access points, 18
DEVICE.XML, 64
discover devices
    cannot discover a client, 54
    cannot discover an access point, 34
    clients, 49

networks or access points, 23

–E–

enable 2.4 GHz or 5 GHz band, 17

–F–

files
- ACP, 64
- ACS, 64
- delete, 63
- profiles, 14
- rename, 63
- sessions, 62
- transfer to a PC, 65
- XML, 64

flagged device, 22
Fluke Networks
- contact, 2
- Knowledge Base, 1

frequency bands, 17

–G–

g, 26
Gray inaudible access points, 18
Group virtual access points, 18
guard interval, 38
guest device, 22

–H–

help (contact Fluke Networks), 2
Hidden, 25, 29, 51
home screen, 13

–I–

interference
- note, 35
- on usage graph, 40

–K–

keys, 5
Knowledge Base, 1

–L–

Language, 19
LEDs, 5
locate an access point or client
- use the internal antenna, 54

lock icons
- access points screen, 30, 51
- networks screen, 25

log
    messages, 79
    screen, 45

–M–

maintenance, 65
Manage 802.11 settings, 17, 18
memory, 64

–N–

n, 26
n40+, n40-, 26
neighbor device, 22
networks
    connect to a network, 42
    list, 25
    ping, 46
    security credentials, 14
notes, 35
    (...), 26, 30

–O–

options, 67

–P–

password
    network, 14
    profiles, 14
ping
    any address, 46
    default addresses, 44
power
    auto shutoff, 19
    battery, 6
    cannot turn off, 67
power levels for transmission, 20
probe request frames
    from network clients, 49
    from the tester, 17
profile, 14

–R–

registration, 1

–S–

safety information, 2, 65
save a file
    profile, 15
    test session, 62
security credentials, 14, 42

session files
save, 62
settings, 14
802.11, 17
minimum, 7
restore defaults, 67, 83
SNR, 44
SNXXXXXX.ACS, 64
software update, 66
sort a list, 26, 51
specifications, 69
streams, 38

–T–

thresholds for bar graph colors, 21
time, 19
timestamp
access points list, 29
networks list, 25
transfer files to a PC, 65
Transmit probes, 17

–U–

unauthorized device, 22
update the software, 66
User Offsets, 61

–V–

virtual access point, 18

–W–

world mode, 20

–X–

XML files, 64